

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Seigo KOTANI

Application No.:

Group Art Unit:

Filed: October 31, 2003

Examiner:

For: SAFETY JUDGMENT METHOD, SAFETY JUDGMENT SYSTEM, SAFETY  
JUDGMENT APPARATUS, FIRST AUTHENTICATION APPARATUS, AND  
COMPUTER PROGRAM PRODUCT

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)  
herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-323200

Filed: November 6, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date(s) as evidenced by the certified papers attached hereto, in accordance with the  
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: October 31, 2003

By: 

H. J. Staas

Registration No. 22,010

1201 New York Ave, N.W., Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年11月6日  
Date of Application:

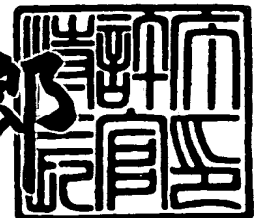
出願番号 特願2002-323200  
Application Number:  
[ST. 10/C]: [JP 2002-323200]

出願人 富士通株式会社  
Applicant(s):

2003年7月9日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3055419

【書類名】 特許願

【整理番号】 0295577

【提出日】 平成14年11月 6日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00  
G06F 17/60 222

【発明の名称】 安全性判断方法、安全性判断システム、安全性判断装置  
、第1認証装置及びコンピュータプログラム

【請求項の数】 20

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内

【氏名】 小谷 誠剛

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705356

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 安全性判断方法、安全性判断システム、安全性判断装置、第1認証装置及びコンピュータプログラム

【特許請求の範囲】

【請求項1】 情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第1認証装置または第2認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第1認証装置へ送信する環境情報送信ステップと、

予め前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記情報処理装置から前記第1認証装置へ送信する暗号化情報送信ステップと、

前記第1認証装置により、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記第1認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第1認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

【請求項2】 情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法にお

いて、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、  
受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第1認証装置または第2認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第1認証装置へ送信する環境情報送信ステップと、

前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記第1認証装置から前記情報処理装置へ送信する暗号化情報送信ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記第1認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記情報処理装置により、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記復号したソフトウェアを前記情報処理装置にインストールするインストールステップと

を備えることを特徴とする安全性判断方法。

【請求項3】 情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、  
受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第1認証装置または第2認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェア

アの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を、前記第2認証装置から発行を受けた個人鍵で暗号化する暗号化ステップと、

予め前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された環境情報を前記情報処理装置から前記第1認証装置へ送信する暗号化情報送信ステップと、

前記第1認証装置により、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記第1認証装置により、前記復号された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第1認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

【請求項4】 情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第1認証装置へ送信する環境情報送信手段と、

前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第1認証装置へ送信する暗号化情報送信手段とを備え、

前記第1認証装置は、

前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から

取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断システム。

【請求項 5】 前記環境情報送信手段及び暗号化情報送信手段は、収集した環境情報を前記個人鍵で暗号化して、前記電子証明書と共に前記第 1 認証装置へ送信するよう構成してあることを特徴とする請求項 4 に記載の安全性判断システム。

【請求項 6】 前記情報処理装置との間で商取引に関する情報を送受信する店舗コンピュータをさらに備え、

前記情報処理装置は、商品情報または金額情報を含む商取引に関する情報を受け付ける手段をさらに備え、

前記暗号化情報送信手段は、前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化された前記商取引に関する情報を前記第 1 認証装置へ送信するよう構成してあり、

前記環境情報認証手段は、送信された商品情報または金額情報に対応する階級に係る環境条件を環境情報データベースから読み出し、該読み出した環境条件に前記送信された環境情報が合致するか否かにより、適正であるか否かを判断するよう構成してあり、

前記第 1 認証装置は、前記安全判断手段により前記情報処理装置が安全と判断した場合に、該情報処理装置の安全性に関する情報を前記店舗コンピュータへ送信する手段をさらに備えることを特徴とする請求項 4 に記載の安全性判断システム。

【請求項 7】 前記第 1 認証装置は、  
生体情報を受け付ける副生体情報受付手段と、



受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、  
接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集手段と、

前記第2認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収集した環境情報を暗号化する副暗号化手段と、

前記第2認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、

前記情報処理装置は、

前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する副環境情報認証手段と、

前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段による認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に、前記情報処理装置及び前記第1認証装置を安全と判断する副安全判断手段とを備えることを特徴とする請求項4に記載の安全性判断システム。

【請求項8】 情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第1認証装置へ送信する環境情報送信手段とを備え、

前記第1認証装置は、

前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフ

トウェアを前記情報処理装置へ送信する暗号化情報送信手段とを備え、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記情報処理装置は、

前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記復号したソフトウェアをインストールするインストール手段とをさらに備える

ことを特徴とする安全性判断システム。

【請求項9】 前記情報処理装置は、主電力供給手段と、副電力供給手段と、副電力供給手段から電力の供給をうける受信用通信手段と、前記主電力供給手段による電力の供給が行われていない場合に、前記暗号化情報送信手段により送信された電子証明書及び個人鍵で暗号化されたソフトウェアを前記受信用通信手段により受信して蓄積する蓄積手段とをさらに備えることを特徴とする請求項8に記載の安全性判断システム。

【請求項10】 前記電子証明書認証手段は、前記主電力供給手段による電力の供給が行われた場合に、前記蓄積手段により蓄積した電子証明書及びソフトウェアを読み出し、前記第2認証装置から取得した公開鍵を用いて、前記電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断するよう構成してあることを特徴とする請求項9に記載の安全性判断システム。

【請求項11】 前記ソフトウェアは、前記情報処理装置に予めインストールされているソフトウェアのパッチ用ソフトウェアであることを特徴とする請求項8乃至10に記載の安全性判断システム。

【請求項12】 前記情報処理装置は、前記インストール手段によりインストールしたソフトウェアを実行した場合、所定の日時以降に記憶部に記憶された

データを消去する消去手段をさらに備えることを特徴とする請求項 8 乃至 10 に記載の安全性判断システム。

【請求項 13】 情報処理装置、第 1 認証装置及び第 2 認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

前記第 2 認証装置から発行を受けた個人鍵で前記生体情報受付手段により受け付けた生体情報及び前記環境情報収集手段により収集した環境情報を暗号化する暗号化手段と、

前記第 2 認証装置から発行を受けた電子証明書及び前記暗号化された生体情報及び環境情報を前記第 1 認証装置へ送信する暗号化情報送信手段とを備え、

前記第 1 認証装置は、

前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された生体情報及び環境情報を復号し、復号された生体情報及び環境情報が適正であるか否かを判断する電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記復号された生体情報と、予め記憶された生体情報とを比較して適正であるか否かを判断する生体情報認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断システム。

【請求項 14】 前記環境情報は、インストールされたソフトウェアの名称またはバージョン、接続された周辺機器の機器名またはバージョン、または、前記情報処理装置の装置名またはバージョンの情報を含むことを特徴とする請求項

4乃至13のいずれかに記載の安全性判断システム。

【請求項15】 前記生体情報は、音声、指紋、網膜、または虹彩の情報であることを特徴とする請求項4乃至14のいずれかに記載の安全性判断システム。

【請求項16】 第1認証装置及び第2認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第1認証装置へ送信する環境情報送信手段と、

前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第1認証装置へ送信する暗号化情報送信手段と、

前記生体情報認証手段により適正と判断され、また前記環境情報送信手段により送信した環境情報が前記第1認証手段により適正と判断され、かつ、前記暗号化情報送信手段により送信した電子証明書及び暗号化された情報が前記第1認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断装置。

【請求項17】 第1認証装置及び第2認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第1認証装置へ送信する環境情報送信手段と、

前記第1認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第2認証装置から取得した公開鍵を用いて電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段及び電子証明書認証手段による認証が適正であると判断

され、また前記環境情報送信手段により送信した環境情報が前記第 1 認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置に前記復号したソフトウェアをインストールするインストール手段とを備えることを特徴とする安全性判断装置。

【請求項 18】 通信網を介して接続される情報処理装置の安全性を判断する第 1 認証装置において、

前記情報処理装置により受け付けた生体情報が適正であるか否かの認証情報を受信する認証情報受信手段と、

通信網を介して接続された第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報が、前記情報処理から送信された場合に、前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、

前記情報処理装置から、該情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を受信した場合に、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、受信した環境情報が適正であるか否かを判断する環境情報認証手段と、

前記認証情報受信手段により、生体情報が適正であるとの認証情報を受信し、また前記環境情報認証手段及び電子証明書認証手段による認証が適正であると判断した場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする第 1 認証装置。

【請求項 19】 第 1 認証装置及び第 2 認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第 1 認証装置へ送信させる環境情

報送信ステップと、

コンピュータに、前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第1認証装置へ送信させる暗号化情報送信ステップと、

コンピュータに、前記生体情報認証ステップにより適正と判断され、また前記環境情報送信ステップにより送信された環境情報が前記第1認証装置により適正と判断され、かつ、前記暗号化情報送信ステップにより送信された電子証明書及び暗号化された情報が前記第1認証装置により適正と判断され、前記第1認証装置から適正であることを示す情報を受信した場合に、コンピュータを安全と判断する安全判断ステップと

を実行させることを特徴とするコンピュータプログラム。

【請求項20】 第1認証装置及び第2認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第1認証装置へ送信させる環境情報送信ステップと、

コンピュータに、前記第1認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第2認証装置から取得した公開鍵を用いて、電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号させ、復号されたソフトウェアが適正であるか否かを判断させる電子証明書認証ステップと、

コンピュータに、前記生体情報認証ステップ及び電子証明書認証ステップによる認証が適正であると判断し、また、前記環境情報送信ステップにより送信した環境情報が前記第1認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記コンピュータに前記復号したソフトウェアをインストールするインストールステップと

を実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法、安全性判断システム、安全性判断装置、第1認証装置及びコンピュータを安全性判断装置として機能させるためのコンピュータプログラムに関し、特に、携帯電話機、家電機器、パーソナルコンピュータ等の情報処理装置に組み込んで、該情報処理装置の安全性を判断する安全性判断装置等に関する。

## 【0002】

## 【従来の技術】

I P v 6 (Internet Protocol Version 6) の導入により、インターネット等の通信網に接続される情報処理装置は、パーソナルコンピュータ、サーバコンピュータ、及び携帯電話機だけではなく、冷蔵庫、電子レンジ、エアコン、TV、DVD等の家電機器、コピー機、さらにはロボット等も通信網に接続され、情報の送受信が行われることになる。このように通信網に接続される情報処理装置が増加するにつれ、安全性（セキュリティ）が低下することになる。

## 【0003】

特に家電機器は安全性が低く、外部から機器の正常な動作に支障をきたすプログラムを送り込まれるケースや、DDoS (Distributed Denial of Service) の踏み台にされる虞がある。そこで、このような情報処理装置の安全性を高めるために、指紋等を用いたバイオメトリック認証機能を情報処理装置に搭載する試みがなされている（例えば、引用文献1）。

## 【0004】

## 【特許文献1】

特開平3-58174号公報

## 【0005】

## 【発明が解決しようとする課題】

しかしながら、認証用の指紋情報が流出する場合もあり、バイオメトリック認証のみでは、高度な安全性を確保することが難しいという問題があった。特にこ

これらの情報処理装置を用いた電子商取引を行う際には、情報処理装置が、正当な所有者が使用しているか、所有者自らの情報処理装置を用いた取引であるか、情報処理装置に安全性を損なう機器が接続、またはOS (Operating System)、ブラウザ、プラグインソフト等のソフトウェアがインストールされていないか等の安全性をまず確保した上で、商取引を行うことが好ましい。

#### 【0006】

また、これらの情報処理装置にパッチ用のソフトウェア、ファームウェア等を提供する場合、第3者に送信中のソフトウェアを改竄される虞があることから、情報送信側の装置と情報処理装置との間での安全性を十分に確保する必要があった。その一方で、安全性のレベルを高めすぎると、円滑な情報の送受信を行うことが困難となる。

#### 【0007】

本発明は斯かる事情に鑑みてなされたものであり、その目的とするところは、生体情報を用いた認証、認証機関を利用した電子証明書による認証 (PKI (Public Key Infrastructure 認証)、及び情報処理装置の利用環境の階級を利用した環境情報を用いた認証を組み合わせることで認証を行うことにより、安全性を高めることができ、また妥当な安全性を維持した上で円滑に情報の送受信を行うことが可能な安全性判断方法、安全性判断システム、安全性判断装置、第1認証装置及びコンピュータを安全性判断装置として機能させるためのコンピュータプログラムを提供することにある。

#### 【0008】

また、本発明の他の目的は、商取引が行われる商品の価値に応じて安全性の階級を変化させることにより、安全性を確保した上で円滑な商取引を実現することが可能な安全性判断システムを提供することにある。

#### 【0009】

さらに、本発明の他の目的は、主電力供給手段とは別の副電力供給手段からの電力供給をうける受信用通信手段をもちいて、パッチ用ソフトウェア等を受信して蓄積しておくことにより、安全性を確保した上で容易にパッチ用ソフトウェア等を配布することが可能な安全性判断システムを提供することにある。



## 【0010】

## 【課題を解決するための手段】

第1発明に係る安全性判断方法は、情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第1認証装置または第2認証装置により判断する生体情報認証ステップと、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、収集した環境情報を前記情報処理装置から前記第1認証装置へ送信する環境情報送信ステップと、予め前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記情報処理装置から前記第1認証装置へ送信する暗号化情報送信ステップと、前記第1認証装置により、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証ステップと、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記第1認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第1認証装置により、前記情報処理装置を安全と判断する安全判断ステップとを備えることを特徴とする。

## 【0011】

第2発明に係る安全性判断方法は、情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第1認証装置または第2認証装置により判断する生体情報認証ステップと、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、収集した環境情報

を前記情報処理装置から前記第 1 認証装置へ送信する環境情報送信ステップと、前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記第 1 認証装置から前記情報処理装置へ送信する暗号化情報送信ステップと、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記第 1 認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、前記情報処理装置により、前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証ステップと、前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記復号したソフトウェアを前記情報処理装置にインストールするインストールステップとを備えることを特徴とする。

#### 【0012】

第 3 発明に係る安全性判断方法は、情報処理装置、第 1 認証装置及び第 2 認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第 1 認証装置または第 2 認証装置により判断する生体情報認証ステップと、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、収集した環境情報を、前記第 2 認証装置から発行を受けた個人鍵で暗号化する暗号化ステップと、予め前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化された環境情報を前記情報処理装置から前記第 1 認証装置へ送信する暗号化情報送信ステップと、前記第 1 認証装置により、前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する電子証明書認証ステップと、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記第 1 認証装置により、前記復号された環境情報が適正であるか否かを判断する環境情報認証ステップと、前

記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第1認証装置により、前記情報処理装置を安全と判断する安全判断ステップとを備えることを特徴とする。

【0013】

第4発明に係る安全性判断システムは、情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、前記情報処理装置は、生体情報を受け付ける生体情報受付手段と、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第1認証装置へ送信する環境情報送信手段と、前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第1認証装置へ送信する暗号化情報送信手段とを備え、前記第1認証装置は、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段とを備えることを特徴とする。

【0014】

第5発明に係る安全性判断システムは、第4発明において、前記環境情報送信手段及び暗号化情報送信手段は、収集した環境情報を前記個人鍵で暗号化して、前記電子証明書と共に前記第1認証装置へ送信するよう構成してあることを特徴とする。

【0015】

第6発明に係る安全性判断システムは、第4発明において、前記情報処理装置との間で商取引に関する情報を送受信する店舗コンピュータをさらに備え、前記情報処理装置は、商品情報または金額情報を含む商取引に関する情報を受け付け

る手段をさらに備え、前記暗号化情報送信手段は、前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された前記商取引に関する情報を前記第1認証装置へ送信するよう構成してあり、前記環境情報認証手段は、送信された商品情報または金額情報に対応する階級に係る環境条件を環境情報データベースから読み出し、該読み出した環境条件に前記送信された環境情報が合致するか否かにより、適正であるか否かを判断するよう構成してあり、前記第1認証装置は、前記安全判断手段により前記情報処理装置が安全と判断した場合に、該情報処理装置の安全性に関する情報を前記店舗コンピュータへ送信する手段をさらに備えることを特徴とする。

#### 【0016】

第7発明に係る安全性判断システムは、第4発明において、前記第1認証装置は、生体情報を受け付ける副生体情報受付手段と、受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集手段と、前記第2認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収集した環境情報を暗号化する副暗号化手段と、前記第2認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、前記情報処理装置は、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証手段と、送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する副環境情報認証手段と、前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段による認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に、前記情報処理装置及び前記第1認証装置を安全と判断する副安全判断手段とを備えることを特徴とする。

#### 【0017】

第8発明に係る安全性判断システムは、情報処理装置、第1認証装置及び第2

認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、前記情報処理装置は、生体情報を受け付ける生体情報受付手段と、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第 1 認証装置へ送信する環境情報送信手段とを備え、前記第 1 認証装置は、前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記情報処理装置へ送信する暗号化情報送信手段とを備え、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、前記情報処理装置は、前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記復号したソフトウェアをインストールするインストール手段とをさらに備えることを特徴とする。

#### 【0018】

第 9 発明に係る安全性判断システムは、第 8 発明において、前記情報処理装置は、主電力供給手段と、副電力供給手段と、副電力供給手段から電力の供給を受ける受信用通信手段と、前記主電力供給手段による電力の供給が行われていない場合に、前記暗号化情報送信手段により送信された電子証明書及び個人鍵で暗号化されたソフトウェアを前記受信用通信手段により受信して蓄積する蓄積手段とをさらに備えることを特徴とする。

#### 【0019】

第 10 発明に係る安全性判断システムは、第 9 発明において、前記電子証明書認証手段は、前記主電力供給手段による電力の供給が行われた場合に、前記蓄積手段により蓄積した電子証明書及びソフトウェアを読み出し、前記第 2 認証装置から取得した公開鍵を用いて、前記電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断す

るよう構成してあることを特徴とする。

【0020】

第11発明に係る安全性判断システムは、第8発明乃至第10発明のいずれかにおいて、前記ソフトウェアは、前記情報処理装置に予めインストールされているソフトウェアのパッチ用ソフトウェアであることを特徴とする。

【0021】

第12発明に係る安全性判断システムは、第8発明乃至第10発明のいずれかにおいて、前記情報処理装置は、前記インストール手段によりインストールしたソフトウェアを実行した場合、所定の日時以降に記憶部に記憶されたデータを消去する消去手段をさらに備えることを特徴とする。

【0022】

第13発明に係る安全性判断システムは、情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、前記情報処理装置は、生体情報を受け付ける生体情報受付手段と、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、前記第2認証装置から発行を受けた個人鍵で前記生体情報受付手段により受け付けた生体情報及び前記環境情報収集手段により収集した環境情報を暗号化する暗号化手段と、前記第2認証装置から発行を受けた電子証明書及び前記暗号化された生体情報及び環境情報を前記第1認証装置へ送信する暗号化情報送信手段とを備え、前記第1認証装置は、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された生体情報及び環境情報を復号し、復号された生体情報及び環境情報が適正であるか否かを判断する電子証明書認証手段と、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、前記復号された生体情報と、予め記憶された生体情報とを比較して適正であるか否かを判断する生体情報認証手段と、前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段とを備える

ことを特徴とする。

【0023】

第14発明に係る安全性判断システムは、第4発明乃至第13発明のいずれかにおいて、前記環境情報は、インストールされたソフトウェアの名称またはバージョン、接続された周辺機器の機器名またはバージョン、または、前記情報処理装置の装置名またはバージョンの情報を含むことを特徴とする。

【0024】

第15発明に係る安全性判断システムは、第4発明乃至第14発明のいずれかにおいて、前記生体情報は、音声、指紋、網膜、または虹彩の情報であることを特徴とする。

【0025】

第16発明に係る安全性判断装置は、第1認証装置及び第2認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第1認証装置へ送信する環境情報送信手段と、前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第1認証装置へ送信する暗号化情報送信手段と、前記生体情報認証手段により適正と判断され、また前記環境情報送信手段により送信した環境情報が前記第1認証手段により適正と判断され、かつ、前記暗号化情報送信手段により送信した電子証明書及び暗号化された情報が前記第1認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置を安全と判断する安全判断手段とを備えることを特徴とする。

【0026】

第17発明に係る安全性判断装置は、第1認証装置及び第2認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報

を含む環境情報を収集する環境情報収集手段と、収集した環境情報を前記第1認証装置へ送信する環境情報送信手段と、前記第1認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第2認証装置から取得した公開鍵を用いて電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、前記生体情報認証手段及び電子証明書認証手段による認証が適正であると判断され、また前記環境情報送信手段により送信した環境情報が前記第1認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置に前記復号したソフトウェアをインストールするインストール手段とを備えることを特徴とする。

#### 【0027】

第18発明に係る第1認証装置は、通信網を介して接続される情報処理装置の安全性を判断する第1認証装置において、前記情報処理装置により受け付けた生体情報が適正であるか否かの認証情報を受信する認証情報受信手段と、通信網を介して接続された第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報が、前記情報処理から送信された場合に、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、前記情報処理装置から、該情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を受信した場合に、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、受信した環境情報が適正であるか否かを判断する環境情報認証手段と、前記認証情報受信手段により、生体情報が適正であるとの認証情報を受信し、また前記環境情報認証手段及び電子証明書認証手段による認証が適正であると判断した場合に前記情報処理装置を安全と判断する安全判断手段とを備えることを特徴とする。

#### 【0028】

第19発明に係るコンピュータプログラムは、第1認証装置及び第2認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュ



タプログラムにおいて、コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、コンピュータに、収集させた環境情報を前記第1認証装置へ送信させる環境情報送信ステップと、コンピュータに、前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第1認証装置へ送信させる暗号化情報送信ステップと、コンピュータに、前記生体情報認証ステップにより適正と判断され、また前記環境情報送信ステップにより送信された環境情報が前記第1認証装置により適正と判断され、かつ、前記暗号化情報送信ステップにより送信された電子証明書及び暗号化された情報が前記第1認証装置により適正と判断され、前記第1認証装置から適正であることを示す情報を受信した場合に、コンピュータを安全と判断する安全判断ステップとを実行させることを特徴とする。

#### 【0029】

第20発明に係るコンピュータプログラムは、第1認証装置及び第2認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、コンピュータに、収集させた環境情報を前記第1認証装置へ送信させる環境情報送信ステップと、コンピュータに、前記第1認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第2認証装置から取得した公開鍵を用いて、電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号させ、復号されたソフトウェアが適正であるか否かを判断させる電子証明書認証ステップと、コンピュータに、前記生体情報認証ステップ及び電子証明書認証ステップによる認証が適正であると判断し、また、前記環境情報送信ステップにより送信した環境情報が前記第1認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記コンピュータに前記復号したソフトウェアをインストールするインストールステップとを実行させることを特

徴とする。

#### 【0030】

本発明にあつては、利用者の指紋等の生体情報を受け付け、受け付けた生体情報が適正であるか否かを判断する。また、情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する。具体的には、情報処理装置自身の機器名、バージョン、情報処理装置に接続されている機器の名称、インストールされているブラウザ名、OS名、バージョン等の情報が該当する。情報処理装置は収集した環境情報を第1認証装置へ送信する。

#### 【0031】

さらに、第3者的な立場にある認証機関等の第2認証装置から発行を受けた電子証明書及び情報処理装置の個人鍵で暗号化された商取引に関する情報等を第1認証装置へ送信する。第1認証装置は、電子証明書及び暗号化された情報を受信した場合、第2認証装置から取得した第2認証装置（認証機関）の公開鍵を用いて、送信された電子証明書から情報処理装置の公開鍵を取得する。そして、取得した情報処理装置の公開鍵で暗号化された情報を復号し、復号された情報が適正であるか否かをメッセージダイジェストなどを用いて判断する。

#### 【0032】

第1認証装置は、送受信される情報に応じて階級付けされた環境情報の条件を記憶した環境情報データベース及び送信された情報を参照して、送信された環境情報が適正であるか否かを判断する。つまり、送受信される情報に対して高度な安全性を確保する必要がある場合、情報処理装置の環境情報は、より条件の厳しい（階級の高い）環境条件を満たす必要がある。例えば、高度な安全性が必要とされる場合（例えば、株取引、5万円以上の高額商品の取引）は、情報処理装置のOSが最新のバージョンであることを条件としておき、情報処理装置のOSが最新のバージョンである場合は、環境認証が適正であると判断し、情報処理装置のOSが最新のバージョンでない場合（旧バージョンのOSの場合など）は、セキュリティホールがある虞があるので、環境認証が適正でないと判断する。

#### 【0033】

一方、低価格商品の取引の場合、安全性よりも利便性を確保する必要があるの

で、高い階級の条件を満たす必要はなく、多少セキュリティホールのあるバージョンの古いOSをインストールしている場合でも環境認証が適正であると判断させる。例えば、100円程度の、商品の取引の場合は、情報処理装置のOSが旧バージョンであったとしても環境認証が適正であると判断する。そして、生体情報認証、環境情報認証、及び電子証明書認証による認証が全て適正である場合に情報処理装置を安全と判断する、例えば安全であることを示すフラグをセットし、安全であることを示す情報を、商取引を行う店舗コンピュータへ通知し、安全性を確保した上で情報処理装置と店舗コンピュータとの間の、情報の送受信を行う。このように構成したので、情報処理装置の安全性を確保しつつ、円滑な情報の送受信及び商取引を実現することが可能となる。さらに、第1認証装置においても生体情報認証、電子証明書認証及び環境認証をおこない、情報処理装置における生体情報認証、電子証明書認証及び環境認証、並びに、第1に認証装置における生体情報認証、電子証明書認証及び環境認証において、全て適正と判断された場合のみ、第1認証装置及び情報処理装置の双方を安全と判断するようにしたので、さらに高度な安全性を確保することが可能となる。

#### 【0034】

また、本発明にあつては、利用者の指紋等の生体情報を受け付け、受け付けた生体情報が適正であるか否かの本人認証を行う。そして上述したように情報処理装置は収集した環境情報を第1認証装置へ送信し、第1認証装置において、環境情報の認証を行う。第1認証装置から情報処理装置へパッチ用のソフトウェア等を送信する場合は、第1認証装置は、第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを情報処理装置へ送信する。

#### 【0035】

前記情報処理装置は、電子証明書及び暗号化されたソフトウェアを受信した場合、第2認証装置へ公開鍵を要求し、この認証機関の公開鍵を用いて電子証明書から第1認証装置の公開鍵を取得する。そしてこの公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する。最後に、上述した本人認証、環境認証及び電子証明書による認証が全て適正であると判断した場合、復号したソフトウェアを情報処理装置へインストールする。この

ように構成したので、第3者のなりすましを防止でき、高度な安全性を維持した上で情報処理装置へパッチ用のソフトウェア、ファームウェア等のソフトウェアを提供することが可能となる。

#### 【0036】

さらに、本発明にあつては、情報処理装置は、主電力供給手段及び副電力供給手段を備え、受信用通信手段は副電力供給手段から電力の供給をうける構成としている。主電力供給手段による電力の供給が行われていない場合、すなわちメインの電源がオンにされていない場合に、第1認証装置から電子証明書及び個人鍵で暗号化されたソフトウェアが送信された場合は、サブバッテリーを用いた受信用通信手段によりこれらの情報を受信して蓄積する。そして、主電力供給手段による電力の供給が行われた場合に、蓄積した電子証明書及びソフトウェアを読み出し、送信されたソフトウェアが適正であるか否かの判断、本人認証及び環境認証を行うようにしたので、電源をオンにしていない顧客に対してもパッチ用のソフトウェアを、安全性を確保した上で大量に配布することが可能となる。また特に提供するソフトウェアとして、所定の日時以降に記憶されたデータを記憶部から消去するソフトウェアを提供することによりDDoS攻撃の踏み台にされることを効果的に防止することが可能となる。

#### 【0037】

##### 【発明の実施の形態】

以下本発明を実施の形態を示す図面に基づいて詳述する。

##### 実施の形態1

実施の形態1では、情報処理装置を携帯電話機であるものとし、本発明に係る安全性判断システムを、携帯電話機を用いた商取引に適用した場合について説明する。なお、情報処理装置は携帯電話機に限定されるものではなく、パーソナルコンピュータ、コピー機、プリンタ、FAX、冷蔵庫、TV、DVDプレーヤ、PDA(Personal digital Assistant)、空気調和機、電子レンジ、ロボット等であっても良い。

#### 【0038】

図1は本発明に係る安全性判断システムの概要を示す模式図である。図におい

て1は情報処理装置としての携帯電話機、3は電子証明書の発行を行う第3者の立場にある認証機関の第2認証装置（以下、認証機関サーバという）、2は安全性判断局であって携帯電話機1の安全性を判断する第1認証装置としての中央サーバ、4はオンラインでの商品の販売処理を行うオンラインショップの店舗コンピュータ（以下、Webサーバという）である。携帯電話機1は図示しない携帯電話網を介して、通信網（以下、インターネットという）Nに接続されており、同様に認証機関サーバ3、中央サーバ2、及びWebサーバ4もインターネットNに接続されている。携帯電話機1には生体情報受付手段として指紋取得部112が設けられており、顧客の指紋をスキャンして携帯電話機1に取り込む機能を有する。

#### 【0039】

図2は携帯電話機1のハードウェア構成を示すブロック図である。情報処理装置としての携帯電話機1は通話、文字、画像データの送受信等、通常の機能を果たす携帯電話機エンジン部110及び本発明に係る安全性判断装置5から構成される。本実施の形態においては、安全性判断装置（以下、セキュリティチップという）5はLSI（Large Scale Integrated Circuit）チップであり、携帯電話機1の内部に実装される。

#### 【0040】

以下に、携帯電話機エンジン部110のハードウェア構成について説明する。図に示すように、CPU(Central Processing Unit)11にはバス17を介してRAM12、ROM15、アンテナ部16、電源部113、マイク・スピーカ111、AD/DA112、外部接続端子19、データ表示用の液晶ディスプレイ等の表示部14、及び数字キー、カーソルキー、選択確定キー等から構成される入力部13等が接続される。CPU11は、バス17を介して携帯電話機1の上述したようなハードウェア各部と接続されていて、それらを制御すると共に、ROM15に格納された制御プログラム15Pに従って、種々のソフトウェア的機能を実行する。

#### 【0041】

外部接続端子19は例えば16芯からなるインターフェースであり、USBケ

ーブル等を介して、図示しないパーソナルコンピュータ、または周辺機器と接続される。RAM 12は、SRAM(Static Random Access Memory)またはフラッシュメモリ等で構成され、ソフトウェアの実行時に発生する一時的なデータを記憶する。ROM 15は例えばEEPROM(Electrically Erasable and Programmable ROM)等で構成され、携帯電話機1の基本的操作環境を提供するOS(Operating System)、外部接続端子19に接続された周辺機器等を制御するBIOS(Basic Input/Output System)、及びダウンロードまたは予めインストールされているJava(登録商標)等のソフトウェアが記憶されている。

#### 【0042】

携帯電話機エンジン部110の入力部13とは別に、顧客の指紋を取得する指紋取得部112が携帯電話機1の入力部13の近傍に設けられている。指紋取得部112はスキャンして読み取った指紋データをセキュリティチップ5へ出力する。なお、本実施の形態においては生体情報として指紋を用いることとしたが、これに限るものではなく、音声、網膜、または虹彩等の情報であっても良い。例えば、音声の場合マイク・スピーカ111から音声を取得し、音声をAD/DA112を用いて電気信号に変換し、CPU11へ出力し、予め記憶してある顧客本人の音声データと比較することにより認証を行う。

#### 【0043】

次に、セキュリティチップ5のハードウェア構成について説明する。セキュリティチップ5は、マイクロプロセッサ(以下、MPUという)51、RAM52、EEPROM等のROM55を備えている。MPU51は、バス57を介して上述したRAM52及びROM55と接続されていて、それらを制御すると共に、ROM55に格納された制御プログラム55Pに従って、種々のソフトウェア的機能を実行する。ROM55には、認証機関サーバ3から受信した電子証明書を記憶する電子証明書ファイル553、携帯電話機1自身の個人鍵を記憶する個人鍵ファイル554、予め顧客の指紋情報を記憶した指紋情報ファイル552、及び、携帯電話機1の機器名・バージョン、周辺機器の機器名・バージョン、インストールされているソフトウェアのソフト名・バージョン等を記憶した環境情報ファイル551が用意されている。なお、携帯電話機1の個人鍵は認証機関サ

サーバ3により発行され、この個人鍵と対になる携帯電話機1の公開鍵は任所機関サーバ3が管理している。

#### 【0044】

セキュリティチップのMPU51は携帯電話機1の環境情報を収集して環境情報ファイル551に環境情報を記憶する。MPU51は、予め記憶されている携帯電話機1の機器名・バージョンをROM151から取得し、携帯電話機1自身の情報を取得する。例えば、情報処理装置が携帯電話機である場合、機器名・バージョン、情報処理装置が電子レンジである場合、メーカー名、機器名、型番等を取得する。また、MPU51は、ROM17のBIOSを参照して、外部接続端子19に接続された機器の情報を取得して環境情報の一つとして環境情報ファイル551に記憶する。例えば、図示しないコンピュータが外部接続端子19に接続された場合、コンピュータの機器名等が取得される。また情報処理装置がパーソナルコンピュータである場合に、外部接続端子19としてのPCカードスロットにPCカードが接続された場合は、該PCカードの機器名等を取得する。

#### 【0045】

環境情報としてはさらに、携帯電話機1にインストールされているソフトウェアの情報が該当する。MPU51はROM15のOS及びソフトウェアを参照し、インストールされているソフトウェアの名称及びバージョンを取得する。例えば、情報処理装置がパーソナルコンピュータである場合、OSの名称としてウィンドウズ（登録商標）またはLinux、バージョンとしてSecond Edition等の環境情報が取得され、インストールされているソフトウェアとしてブラウザのインターネットエクスプローラ（登録商標）、バージョンとしてSP2等の情報が取得される。その他、インターネットNを通じてダウンロードしたJava（登録商標）等で記述されたソフトウェアの名称などが該当する。このようにMPU51はROM内のBIOS、OS等を常時監視しており、新たなソフトウェアがインストールされた場合、または外部接続端子19に新たな機器が接続された場合、環境情報としてそれらの情報を収集して環境情報ファイル551に記憶する。

#### 【0046】

指紋情報ファイル 552 は本人認証のために用いるものであり、例えば携帯電話機 1 の購入時に、店舗において顧客の指紋を取得し ROM 55 内の指紋情報ファイル 552 に初期登録する。MPU 51 は指紋取得部 112 から、指紋情報が読み取られて出力された場合は、出力された指紋情報と指紋情報ファイル 552 に記憶した指紋情報とを比較して適正か否かを判断する。なお、本実施の形態においては認証に用いる指紋情報ファイル 552 を携帯電話機 1 に設けることとしているが、これに限るものではなく、中央サーバ 2 または認証機関サーバ 3 等に設け、中央サーバ 2 または認証機関サーバ 3 等で、認証を行うようにしても良い。この場合、個人鍵ファイル 554 の個人鍵で暗号化された指紋情報が電子証明書と共に中央サーバ 2 または認証機関サーバ 3 へ送信され認証が行われる。

#### 【0047】

電子証明書ファイル 553 には認証機関サーバ 3 から発行を受けた電子証明書が記憶されており、また個人鍵ファイル 554 には同じく認証機関サーバ 3 から発行を受けた携帯電話機 1 用の個人鍵が記憶されている。なお、携帯電話機 1 用の公開鍵は認証機関サーバ 3 が記憶している。MPU 51 は送受信される商取引に関するデータ、また環境情報、指紋情報等については、メッセージダイジェスト共に個人鍵で暗号化し、暗号化データと電子証明書とをインターネット N を介して中央サーバ 2 等に送信する。

#### 【0048】

図 3 は中央サーバ 2 のハードウェア構成を示すブロック図である。図に示すように、CPU (Central Processing Unit) 21 にはバス 27 を介して RAM 22、ハードディスク等の記憶部 25、携帯電話機 1、認証機関サーバ 3 及び Web サーバ 4 等と情報を送受信するためのゲートウェイ、LAN カード等の通信部 26、液晶ディスプレイ等の表示部 24、及びキーボード、マウス等の入力部 23 が接続される。CPU 21 は、バス 27 を介して中央サーバ 2 の上述したようなハードウェア各部と接続されていて、それらを制御すると共に、記憶部 25 に格納された制御プログラム 25P に従って、種々のソフトウェア的機能を実行する。また、記憶部 25 には送受信される情報の安全性の階級に応じて環境条件が記憶された環境情報データベース（以下、環境情報 DB という）251 が設けられ



ている。

#### 【0049】

図4は環境情報DB251のレコードレイアウトを示す説明図である。図に示すように階級に応じて環境情報の条件が記憶されている。階級フィールドは送受信される情報の安全性の重要度に応じて1～6に階級付けされており、階級1が最も安全性のレベルが高く、階級6が安全性のレベルが最も低いことを示す。金額情報フィールド及び商品情報フィールドに示すように、100円程度の少額の取引、または商品が着信メロディ（以下、着メロという）等の価格の低い商品等の場合は、安全性よりも円滑な取引を重視する必要があることから、階級が6とされている。一方、50000円以上の高額商品の取引である場合、商品が株券等の場合は、高い安全性を確保する必要があるので階級が1とされている。

#### 【0050】

環境条件フィールド中の装置情報フィールドには顧客の携帯電話機1の機器名・バージョンが階級に対応づけられて記憶されている。例えば、階級1の場合、最新機種であるS004、F004、及びN004である携帯電話機1であることが条件とされており、環境情報としてこの条件を満たさない限り環境認証において適正と判断されない。特にS004については、携帯電話機1のバージョンが2.0以上であることも条件とされている。これに対し、階級6の場合、古い機種であるS001を含め、S001、S002、S003及びS004の他、同様にF001～F004、並びにN001～N004の携帯電話機1であれば、適正と判断される。

#### 【0051】

周辺機器フィールドも同様に階級毎に周辺機器の機器名及びバージョンが記憶されており、環境認証に利用される。例えば、階級6の場合は、周辺機器XX、XY等が接続されている場合でも、環境認証において適正と判断される。その一方で階級1の場合は、対応する周辺機器の条件が記憶されておらず、環境情報として携帯電話機1から、周辺機器の情報が送信された場合は、適正と判断されない。すなわち階級1の場合はいかなる周辺機器が接続されていても環境認証において不適正と判断される。なお、これらの情報は各ベンダーから提供されるもの

を記憶している。

#### 【0052】

同じくソフトウェアフィールドも階級に応じてソフトウェア名及びバージョンが記憶されている。階級6ではソフトウェアCであって、バージョンが3.0以上の場合に適正と判断される。その一方で、階級6の場合はソフトウェアCであってバージョンが1.0以上であれば適正と判断される。このように階級を設けて安全性を判断したのは、円滑な商取引と安全性の維持とのバランスを考慮したものである。例えば、情報処理装置がパーソナルコンピュータである場合、インストールされるブラウザは顧客によって異なる。例えば、マイクロソフト（登録商標）社のインターネットエクスプローラ（登録商標）では、複数のバージョンが存在し、バージョンが上がるに連れセキュリティホールが存在が少なくなっている。

#### 【0053】

高度な安全性が要求される場合は、環境情報を取得して、セキュリティホールのない最新のバージョンのブラウザである場合にのみ適正であると判断し、以降の商取引を許可することも考えられるが、そうすると、最新のバージョンをインストールしていない顧客は全く商取引を行うことができず妥当性を欠くことになる。そこで、安全性がそれほど要求されない低額商品等である場合は、認証の階級を低くし、多少バージョン古いブラウザであっても、一定条件下で適正と判断し商取引を認めることとしたものである。

#### 【0054】

以上のハードウェア構成において本発明における安全性判断の処理手順を、フローチャートを用いて説明する。図5はWebサーバ4と携帯電話機1との間の商取引の手順を示すフローチャートである。まず、携帯電話機1の入力部13に商取引を行うオンラインショップのWebサーバ4のURL (Uniform Resource Locator)を入力して、商品発注ページの取得要求をWebサーバ4に対して行う（ステップS51）。HTTP (Hypertext Transfer Protocol) サーバとしてのWebサーバ4は図示しない記憶部から対応するcHTML (compact Hypertext Markup Language) ファイルを読み出し（ステップS52）、読み出したcH

TML ファイルを携帯電話機 1 へ送信する (ステップ S 5 3)。

【0055】

携帯電話機 1 の CPU 11 は受信した cHTML を ROM 15 に記憶したブラウザソフトウェアにて解析し、図 6 の如く商取引の Web ページを表示する (ステップ S 5 4)。図 6 は Web ページのイメージを示す説明図である。図に示すように表示部 14 には発注する商品、数量、及び金額の情報が表示される。顧客は発注する商品及び数量を、入力部 13 を操作して選択する。商品が選択された場合は、CPU 11 は cHTML ファイルと同時に送信された Java スクリプトを実行し合計金額を算出して表示する。本実施の形態におけるオンラインショップは、パーソナルコンピュータ、プリンタ、ディスクドライブ等のコンピュータ関連機器を販売しており、顧客は 29800 円のインクジェットプリンタを 1 台注文する様子を示している。すなわち顧客は商取引に関する注文情報として、金額情報または商品情報を入力する。この他、住所、電話番号、氏名、ID、パスワード等を入力させるようにしても良い。

【0056】

このようにして入力部 13 から注文情報が入力され、CPU 11 はこの注文情報を受け付ける (ステップ S 5 5)。そして、図 6 に示す「発注する」ボタンが選択された場合、安全性の判断処理に移行する (ステップ S 5 6)。なお、ステップ S 5 7 以降の処理については後述する。以下に、本発明の特徴である安全性の判断処理のサブルーチンを、フローチャートを用いて説明する。

【0057】

図 7 乃至図 12 は安全性の判断処理の手順を示すフローチャートである。注文情報が入力された場合、セキュリティチップ 5 の MPU 51 は制御プログラム 55P を実行し、表示部 14 に指紋情報の取得要求を表示する (ステップ S 7 1)。表示する内容は予め ROM 55 に記憶されており、「例えば、指紋取得部に親指をおいて下さい。」等の情報を読み出して表示部 14 へ出力するようにすればよい。指紋取得部 112 から指紋情報が入力された場合、セキュリティチップ 5 の MPU 51 は指紋情報を受け付け (ステップ S 7 2)、RAM 52 に一時的に記憶する。そして、MPU 51 は ROM 55 の指紋情報ファイル 552 に携帯電

話機 1 の購入時に予め記憶してある指紋情報を読み出し、RAM 52 に記憶した指紋情報と比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップ S 73）。

#### 【0058】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップ S 73 で YES）、指紋認証適正フラグをセットし、セットした指紋認証適正フラグを中央サーバ 2 へ送信する（ステップ S 75）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップ S 73 で NO）、指紋認証不適正フラグをセットし、セットした指紋認証不適正フラグを中央サーバ 2 へ送信する（ステップ S 74）。中央サーバ 2 の CPU 21 は送信された指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）を記憶部 25 に記憶する（ステップ S 77）。なお、本実施の形態においては指紋を用いた生体認証を携帯電話機 1 において実行することとしたが、予め採取した指紋情報を認証機関サーバ 3 または中央サーバ 2 に記憶しておき、認証機関サーバ 3 または中央サーバ 2 において判断するようにしても良い。これにより指紋を用いた生体認証が終了する。

#### 【0059】

続いて、電子証明書を用いた認証へ移行する。セキュリティチップ 5 の MPU 51 は、ステップ S 55 で入力された注文情報に、ROM 55 に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップ S 76）。MPU 51 は認証機関サーバ 3 から予め発行を受けた携帯電話機 1 の個人鍵を個人鍵ファイル 554 から読み出し、注文情報及びメッセージダイジェストを暗号化する（ステップ S 81）。さらに、MPU 51 は電子証明書ファイル 553 から認証機関サーバ 3 において予め発行を受けた電子証明書を読み出し、暗号化した注文情報及びメッセージダイジェストに電子証明書を添付して中央サーバ 2 へ送信する（ステップ S 82）。中央サーバ 2 の CPU 21 は送信された電子証明書、暗号化された注文情報及びメッセージダイジェストを RAM 22 に記憶する。

#### 【0060】

中央サーバ 2 の CPU 21 は電子証明書に記載されている認証機関サーバ 3 へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求す

る（ステップS83）。認証機関サーバ3は、電子証明書の公開鍵を中央サーバへ送信する（ステップS84）。中央サーバ2のCPU21は、記憶した電子証明書をRAM22から読み出し、認証機関サーバ3から送信された認証機関の公開鍵を用いて電子証明書を復号し、携帯電話機1の公開鍵を取得する（ステップS85）。

#### 【0061】

中央サーバ2のCPU21は取得した携帯電話機1の公開鍵を用いて暗号化された注文情報及びメッセージダイジェストを復号する（ステップS91）。さらにCPU21は復号した注文情報に、中央サーバ2の記憶部25に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップS92）。中央サーバ2のCPU21はステップS91で復号したメッセージダイジェストと、ステップS92で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある顧客の携帯電話機1から情報が送受信されたものであるか否かを判断する（ステップS93）。

#### 【0062】

メッセージダイジェストが一致しない場合は（ステップS93でNO）、CPU21は何らかの改竄またはなりすましがあつたと判断し、電子証明書認証の不適正フラグをセットする（ステップS95）。一方、メッセージダイジェストが一致する場合は（ステップS93でYES）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップS94）。そして、中央サーバ2のCPU21は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）を記憶部25に記憶する（ステップS96）。これにより、電子証明書を用いた認証が終了する。

#### 【0063】

続いて環境認証について説明する。セキュリティチップ5のMPU51は携帯電話機1の環境情報を取得する（ステップS101）。環境情報の収集は、上述したようにMPU51が携帯電話機1のROM15のOS、BIOS及びインストールされるソフトウェアを常駐して監視し、携帯電話機1の機器名、OSの名称、バージョン、外部接続端子19に接続された周辺機器の機器名、バージョン

、インストールされたブラウザ等のソフトウェアのソフト名、バージョンなどを収集することにより行われる。収集された環境情報は環境情報ファイル 551 に記憶される（ステップ S102）。

#### 【0064】

MPU51は環境情報ファイル 551 から収集した環境情報を読み出して中央サーバ2へ送信する（ステップ S103）。中央サーバ2のCPU21は送信された環境情報をRAM22に記憶する。中央サーバ2のCPU21はステップ S91にて復号した注文情報に対応する階級の読み出しを、環境情報ファイル 251を参照して行う（ステップ S104）。つまり、CPU21は金額情報または商品情報フィールドを参照して、注文情報中の取り引きされる金額または商品等を基に、対応する階級を階級フィールドから読み出す。例えば注文する商品の金額が50000円を超える場合は階級1が選択される。

#### 【0065】

CPU21は読み出した階級に対応する環境情報の条件を環境情報DB251から読み出す（ステップ S105）。つまり、読み出した階級を基に、環境条件フィールドから対応する携帯電話機1の装置名・バージョン、ソフト名・バージョン、周辺機器の機器名・バージョンを読み出す。そして、CPU21は、RAM22に記憶され、受信した環境情報が、読み出した環境情報の条件を満たすか否かを判断する（ステップ S111）。条件を満たさない場合（ステップ S111でNO）（例えば階級が1であり、環境情報としてソフトウェアCのバージョン2.0が送信された場合、バージョン3.0以上という条件を満たさない）、環境認証不適正フラグをセットする（ステップ S112）。一方、条件を満たす場合（ステップ S111でYES）、環境認証適正フラグをセットする（ステップ S113）。例えば、条件として階級が1の場合に、環境情報として「携帯電話機1の装置名が最新機種F004、バージョンは2.0、ソフトウェアはソフトウェアCのバージョン5.0がインストールされており、かつ周辺機器に何も接続されていない」場合、環境が適正であると判断する。中央サーバ2のCPU21は環境認証のフラグ（環境認証適正フラグ、または環境認証不適正フラグ）を記憶部25に記憶する（ステップ S114）。これにより環境認証が終了する

## 【0066】

CPU21は、記憶部25に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステップS115）。全ての適正フラグがセットされている場合（ステップS115でYES）、携帯電話機1を安全なものと判断し安全フラグをセットする（ステップS121）。換言すれば、生体認証、電子証明書認証（PKI認証）、および環境認証の全てにおいて適正と判断された場合に限り携帯電話機1を適正なものであると判断する。中央サーバ2のCPU21は安全であることを示す安全保証情報及び注文情報をWebサーバ4へ送信する（ステップS122）。

## 【0067】

一方、生体認証、電子証明書認証（PKI認証）、および環境認証の内、1つでも不適正フラグがセットされている場合は、不適正フラグをセットする（ステップS123）。この場合CPU21は携帯電話機1が危険であることを示す危険情報をWebサーバ4へ送信し（ステップS124）、安全性判断のサブルーチン（ステップS56）を終了する。

## 【0068】

図5において、Webサーバ4は、携帯電話機1の危険情報を中央サーバ2から受信したか否かを判断する（ステップS57）。危険情報を受信していない場合（ステップS57でNO）、Webサーバ4は安全保証情報及び注文情報を受信したか否かを判断する（ステップS58）。安全保証情報及び注文情報を受信していない場合（ステップS58でNO）、またステップS57においてYESの場合、携帯電話機1は不正の可能性が高いとして、商取引の中止を求める情報を携帯電話機1へ送信する（ステップS59）。一方、安全保証情報及び注文情報を受信した場合（ステップS58でYES）、携帯電話機1の安全性は保証されたものであるものとして、注文の受注を正式に行い、受注を行われたことを示す受注確認情報を携帯電話機1へ送信する（ステップS510）。このように、商取引に先立ち、本人認証、PKI認証及び環境認証を行って十分な安全性を確

保すると共に、取引引きされる商品の価値に応じて認証レベルを変化させることで円滑な商取引を実現することが可能となる。

#### 【0069】

##### 実施の形態2

図13は実施の形態2に係る携帯電話機1のハードウェア構成を示すブロック図である。実施の形態1に係る携帯電話機1を実行させるためのコンピュータプログラムは、本実施の形態2のように携帯電話機1にプレインストールして提供することも、またCD-ROM、MO、メモリーカード等の可搬型記録媒体で提供することも可能である。さらに、コンピュータプログラムを回線経由で搬送波として伝搬させて提供することも可能である。すなわち、セキュリティチップ5を搭載する代わりに、セキュリティチップ5と同様の機能をもつコンピュータプログラムを携帯電話機1のROM15にインストールするようにしても良い。以下に、その内容を説明する。

#### 【0070】

図13に示す携帯電話機1に、生体情報を認証させ、環境情報を収集させ、環境情報を送信させ、暗号化情報を送信させ、安全性を判断させるプログラムが記録された記録媒体1a（CD-ROM、MO、メモリーカード又はDVD-ROM等）が携帯電話機1のROM15にインストールされている。インストールの方法としては、外部接続端子19に接続可能なメモリーカード等の記録媒体1aを挿入し、プログラムをインストールするか、または、中央サーバ2から本発明に係るプログラムをダウンロードする。係るプログラムは携帯電話機1のRAM12にロードして実行される。これにより、上述のような本発明の情報処理装置としての携帯電話機1として機能する。

#### 【0071】

##### 実施の形態3

実施の形態1においては、生体情報の認証をセキュリティチップ5において行うこととしたが、中央サーバ2または認証機関サーバ3において実行しても良い。実施の形態2は、生体情報の認証を中央サーバ2において実行する形態であって、また予めセキュリティポリシーが決定されている場合に、本発明を適用した



形態について説明する。

#### 【0072】

図14は実施の形態3に係る携帯電話機1のハードウェア構成を示すブロック図であり、図15は中央サーバ2のハードウェア構成を示すブロック図である。図14及び図15に示すように生体情報の認証は中央サーバ2で実行するため、認証用の指紋情報ファイル252は携帯電話機1の内部ではなく中央サーバ2の記憶部25に記憶されている。なお、認証用の指紋情報は、認証前に、顧客に店舗、サービスセンター等に来店してもらい、免許証、パスポートなどで本人であることを確認した上で、その場で指紋を読み取るなどして初期登録するようにすればよい。

#### 【0073】

図16乃至図20は実施の形態3に係る安全性の判断処理の手順を示すフローチャートである。まず、セキュリティチップ5のMPU51は以後の通信を行うために、安全性の確認を開始することを示す信号を中央サーバ2へ送信する（ステップS161）。中央サーバ2のCPU21は確認開始信号を受信した場合、通信の安全性の階級を決定する（ステップS162）。この階級の決定にあたっては、予め決定したセキュリティポリシーに従って決定する。例えば、以後行われる通信が、住民票の発行、株取引等、高い安全性が必要とされる場合は階級1と決定され、着メロ、待ち受け画面の画像データ等、安全性がそれほど要求されない場合は、階級6とされる。また公共料金の支払い等においては、中程度の安全性を確保するために階級3と決定する。

#### 【0074】

中央サーバ2のCPU21は階級の決定後、確認開始信号に対する応答信号を携帯電話機1へ送信する（ステップS163）。応答信号を受信した場合、セキュリティチップ5のMPU51は制御プログラム55Pを実行し、表示部14に指紋情報の取得要求を表示する（ステップS164）。表示する内容は予めROM55に記憶されており、「例えば、指紋取得部に親指をおいて下さい。」等の情報を読み出して表示部14へ出力するようにすればよい。指紋取得部112から指紋情報が入力された場合、セキュリティチップ5のMPU51は指紋情報を

受け付け、RAM 52に一時的に記憶する（ステップS165）。

【0075】

そして、セキュリティチップ5のMPU 51は携帯電話機1の環境情報を取得する（ステップS166）。環境情報の収集は、上述したようにMPU 51が携帯電話機1のROM 15のOS、BIOS及びインストールされるソフトウェアを常駐して監視し、携帯電話機1の機器名、OSの名称、バージョン、外部接続端子19に接続された周辺機器の機器名、バージョン、インストールされたブラウザ等のソフトウェアのソフト名、バージョンなどを収集することにより行われる。収集された環境情報は環境情報ファイル551に記憶される（ステップS167）。

【0076】

セキュリティチップ5のMPU 51はRAM 52に記憶した生体情報及び環境情報ファイル551に記憶した環境情報を読み出す（ステップS168）。セキュリティチップ5のMPU 51は、読み出した生体情報及び環境情報に、ROM 55に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップS169）。MPU 51は認証機関サーバ3から予め発行を受けた携帯電話機1の個人鍵を個人鍵ファイル554から読み出し、生体情報及び環境情報並びにメッセージダイジェストを暗号化する（ステップS171）。さらに、MPU 51は電子証明書ファイル553から認証機関サーバ3において予め発行を受けた電子証明書を読み出し、暗号化した生体情報及び環境情報並びにメッセージダイジェストに電子証明書を添付して中央サーバ2へ送信する（ステップS172）。中央サーバ2のCPU 21は送信された電子証明書、暗号化された生体情報及び環境情報並びにメッセージダイジェストをRAM 22に記憶する。なお、本実施の形態においては生体情報及び環境情報の双方を暗号化して送信しているが、生体情報または環境情報のいずれか一方のみを暗号化して送信するようにしても良い。

【0077】

中央サーバ2のCPU 21は電子証明書に記載されている認証機関サーバ3へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求す

る（ステップS173）。認証機関サーバ3は、電子証明書の公開鍵を中央サーバ2へ送信し、中央サーバ2は送信された電子証明書の公開鍵を受信する（ステップS174）。中央サーバ2のCPU21は、記憶した電子証明書をRAM22から読み出し、認証機関サーバ3から送信された認証機関の公開鍵を用いて電子証明書を復号し携帯電話機1の公開鍵を取得する（ステップS175）。

#### 【0078】

中央サーバ2のCPU21は取得した携帯電話機1の公開鍵を用いて暗号化された生体情報及び環境情報並びにメッセージダイジェストを復号する（ステップS181）。さらにCPU21は復号した生体情報及び環境情報に、中央サーバ2の記憶部25に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップS182）。中央サーバ2のCPU21はステップS181で復号したメッセージダイジェストと、ステップS182で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある顧客の携帯電話機1から情報が送受信されたものであるか否かを判断する（ステップS183）。

#### 【0079】

メッセージダイジェストが一致しない場合は（ステップS183でNO）、CPU21は何らかの改竄またはなりすましがあつたと判断し、電子証明書認証の不適正フラグをセットする（ステップS185）。一方、メッセージダイジェストが一致する場合は（ステップS183でYES）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップS184）。そして、中央サーバ2のCPU21は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）を記憶部25に記憶する（ステップS186）。

#### 【0080】

続いて、中央サーバ2のCPU21は指紋情報ファイル252から予め登録された認証用の指紋情報を読み出す（ステップS187）。CPU21は復号した指紋情報と、読み出した認証用の指紋情報とを比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップS191）。

## 【0081】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップS191でYES）、指紋認証適正フラグをセットする（ステップS192）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップS191でNO）、指紋認証不適正フラグをセットする（ステップS193）。中央サーバ2のCPU21は指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）を記憶部25に記憶する（ステップS194）。

## 【0082】

中央サーバ2のCPU21はステップS162で決定した階級に対応する環境情報の条件を環境情報DB251から読み出す（ステップS195）。そして、CPU21は、復号された環境情報が、ステップS195にて読み出された環境情報の条件を満たすか否かを判断する（ステップS196）。条件を満たさない場合（ステップS196でNO）、環境認証不適正フラグをセットする（ステップS198）。一方、条件を満たす場合（ステップS196でYES）、環境認証適正フラグをセットする（ステップS197）。中央サーバ2のCPU21は環境認証のフラグ（環境認証適正フラグ、または環境認証不適正フラグ）を記憶部25に記憶する（ステップS201）。

## 【0083】

CPU21は、記憶部25に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステップS202）。全ての適正フラグがセットされている場合（ステップS202でYES）、携帯電話機1を安全なものと判断し安全フラグをセットする（ステップS203）。換言すれば、生体認証、電子証明書認証（PKI認証）、および環境認証の全てにおいて適正と判断された場合に限り携帯電話機1を適正なものであると判断する。中央サーバ2のCPU21は携帯電話機1またはWebサーバ4に通信を継続することを示す信号を送信する（ステップS204）。

## 【0084】

一方、生体認証、電子証明書認証（PKI認証）、および環境認証の内、1つ

でも不適正フラグがセットされている場合は、不適正フラグをセットする（ステップS205）。この場合CPU21は携帯電話機1またはWebサーバ4に通信を終了することを示す信号を送信する（ステップS206）。

#### 【0085】

##### 実施の形態4

実施の形態4は、パッチ用のソフトウェア、ファームウェアを提供する場合に適用される安全性判断システムに関する。PDA、携帯電話機、冷蔵庫、空気調和機、プリンタ等においては、内蔵されるソフトウェアのバグが発見される場合があり、この場合、パッチ用のソフトウェアを提供する必要がある。また、追加機能を備えるファームウェアを提供する場合もある。実施の形態4では安全性を確保した上でこれらのソフトウェアを顧客に提供することが可能な安全性判断システムについて説明する。

#### 【0086】

図21は実施の形態4に係る携帯電話機1のハードウェア構成を示すブロック図である。図21に示す114は携帯電話機エンジン部110に電力を供給する主電力供給手段（以下、主電源部という）であり、リチウム電池等が用いられる。入力部13の図示しないオンボタンの操作により、主電源部114から携帯電話機エンジン部110及びセキュリティチップ5へ電力が供給され、図示しないオフボタンの操作により、主電源部114から携帯電話機エンジン部110及びセキュリティチップ5への電力が遮断され携帯電話機1の電源が切られる。

#### 【0087】

一方、副電力供給手段（以下、副電源部という）115は、例えばコイン形のリチウム電池が用いられ、主電源部114による携帯電話機エンジン部110及びセキュリティチップ5への電力供給が行われていない場合にでも、蓄積手段としての第2ROM116及び受信通信手段としての副アンテナ部117に電力を供給する。主電源部114により電力が供給されている場合、すなわち携帯電話機の電源がオンの場合に、中央サーバ2からソフトウェアが送信されたときは、該ソフトウェアはアンテナ部16からソフトウェアを受信し、CPU11がROM15にソフトウェアを記憶する。この場合、副電源部115による電力供給は

行われていない。

#### 【0088】

逆に、主電源部114による電力供給がなされていない場合、すなわち携帯電話機1の電源がオフの場合、副電源部115により、副アンテナ部117及び第2ROM116に電源が供給される。そして、中央サーバ2からソフトウェアが送信された場合、副アンテナ部117でソフトウェアを受信し、第2ROM116に受信したソフトウェアを記憶し、主電源による電力が供給された時点で、第2ROM116に記憶したソフトウェアをROM15に書き込む処理を行う。なお、副アンテナ部117は、例えば公知のFM文字多重放送受信モジュールを用いればよい。この場合、中央サーバはFM放送局を介してソフトウェアを含むFM文字放送を発信する。副アンテナ部117であるFM文字多重放送受信モジュールが、FM文字放送を受信した場合、DARC規格の文字コードで記述されたソフトウェアのデータを、C言語、Java等で記述されたソースコードに変換する。最後にセキュリティチップ5のMPU51は本人認証、PKI認証及び環境認証を行った上で、ROM15にソフトウェアをインストールする。

#### 【0089】

図22は中央サーバ2のハードウェア構成を示すブロック図である。図22に示すように記憶部25には、認証機関サーバ3による認証を経たパッチ用のソフトウェア、ファームウェア、プラグインソフト、ワクチン等の数々のソフトウェアが記憶されている。なお、これらのソフトウェアはソフトウェア会社から提供を受けている。電子証明書ファイル253には、予め認証機関サーバ3から発行を受けた中央サーバ2の電子証明書が記憶されており、個人鍵ファイル254にも同じく、予め認証機関サーバ3から発行を受けた中央サーバ2の個人鍵が記憶されている。

#### 【0090】

以上のハードウェア構成において安全性が保証されたソフトウェアの提供処理について、フローチャートを用いて説明する。図23乃至図29は実施の形態4に係るソフトウェア提供処理の手順を示すフローチャートである。まず、中央サーバ2のCPU21は携帯電話機1に発呼するなどして、主電源がオンかオフか

の情報の取得要求を行う（ステップS231）。携帯電話機1は主電源がオンかオフの情報を送信する（ステップS232）。中央サーバ2は主電源がオンであるか否かを判断し（ステップS233）、主電源がオンである場合（ステップS233でYES）、ステップS162で説明した如く安全性の階級を決定する（ステップS234）。この安全性に関しては提供されるソフトウェアの重要度に応じて管理者が決定するようにすればよい。例えばパッチ用ソフトウェアまたはワクチンソフトの場合は安全性を高めるべく階級1と決定され、ゲーム用のソフトウェアなど安全性が低いものは階級6と決定される。

#### 【0091】

中央サーバ2のCPU21は認証開始信号を携帯電話機1へ送信する（ステップS235）。認証開始信号を受信したセキュリティチップ5のMPU51は、制御プログラム55Pを実行し、表示部14に指紋情報の取得要求を表示する（ステップS236）。指紋取得部112から指紋情報が入力された場合、セキュリティチップ5のMPU51は指紋情報を受け付け（ステップS237）、RAM52に一時的に記憶する。そして、MPU51はROM55の指紋情報ファイル552に携帯電話機1の購入時に予め記憶してある指紋情報を読み出し、RAM52に記憶した指紋情報と比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップS241）。

#### 【0092】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップS241でYES）、指紋認証適正フラグをセットする（ステップS243）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップS241でNO）、指紋認証不適正フラグセットする（ステップS242）。MPU51は送信された指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）を記憶部55に記憶する（ステップS244）。

#### 【0093】

次に、セキュリティチップ5のMPU51は携帯電話機1の環境情報を取得する（ステップS245）。収集された環境情報は環境情報ファイル551に記憶される（ステップS246）。MPU51は環境情報ファイル551から収集し

た環境情報を読み出して中央サーバ2へ送信する(ステップS247)。中央サーバ2のCPU21は送信された環境情報をRAM22に記憶する。中央サーバ2のCPU21はステップS162にて決定した階級に対応する環境情報の条件を環境情報DB251から読み出す(ステップS248)。

#### 【0094】

そして、CPU21は、RAM22に記憶され、受信した環境情報が、読み出した環境情報の条件を満たすか否かを判断する(ステップS251)。条件を満たさない場合(ステップS251でNO)、環境認証不適正フラグをセットする(ステップS253)。一方、条件を満たす場合(ステップS251でYES)、環境認証適正フラグをセットする(ステップS252)。中央サーバ2のCPU21は環境認証のフラグ(環境認証適正フラグ、または環境認証不適正フラグ)を記憶部25に記憶し(ステップS254)、携帯電話機1へ送信する(ステップS255)。環境認証のフラグを受信したセキュリティチップ5のMPU51は、環境認証フラグ(環境認証適正フラグ、または環境認証不適正フラグ)を記憶部55に記憶する(ステップS256)。

#### 【0095】

さらに中央サーバ2のCPU21は記憶部25に記憶した提供用のソフトウェアを記憶部25から読み出す(ステップS257)。CPU21は、読み出したソフトウェアに、記憶部25に記憶したハッシュ関数を用いてメッセージダイジェストを算出する(ステップS258)。CPU21は認証機関サーバ3から予め発行を受けた中央サーバ2の個人鍵を個人鍵ファイル254から読み出し、ソフトウェア及びメッセージダイジェストを暗号化する(ステップS259)。CPU21は電子証明書ファイル253から認証機関サーバ3において予め発行を受けた電子証明書を読み出し、暗号化したソフトウェア及びメッセージダイジェストに電子証明書を添付して携帯電話機1へ送信する(ステップS261)。セキュリティチップ5のMPU51は送信された電子証明書、暗号化されたソフトウェア及びメッセージダイジェストをRAM52に記憶する。

#### 【0096】

セキュリティチップ5のMPU51は電子証明書に記載されている認証機関サ



ーバ3へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求する（ステップS262）。認証機関サーバ3は、電子証明書の公開鍵を携帯電話機1へ送信し、セキュリティチップ5のMPU51は送信された公開鍵を受信する（ステップS263）。MPU51は記憶した電子証明書をRAM52から読み出し、認証機関サーバ3から送信された認証機関の公開鍵を用いて電子証明書を復号し中央サーバ2の公開鍵を取得する（ステップS264）。

#### 【0097】

セキュリティチップ5のMPU51は取得した中央サーバ2の公開鍵を用いて、暗号化されたソフトウェア及びメッセージダイジェストを復号する（ステップS265）。さらにMPU51は復号したソフトウェアに、セキュリティチップ5のROM55に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップS266）。MPU51はステップS265で復号したメッセージダイジェストと、ステップS266で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある中央サーバ2から情報が送受信されたものであるか否かを判断する（ステップS271）。

#### 【0098】

メッセージダイジェストが一致しない場合は（ステップS271でNO）、MPU51は何らかの改竄またはなりすましがあったと判断し、電子証明書認証の不適正フラグをセットする（ステップS272）。一方、メッセージダイジェストが一致する場合は（ステップS271でYES）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップS273）。そして、セキュリティチップ5のMPU51は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）をROM55に記憶する（ステップS274）。

#### 【0099】

MPU51はROM55に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステ

ップS 275)。全ての適正フラグがセットされている場合(ステップS 275でYES)、送信されたソフトウェアを安全なものと判断し安全フラグをセットする(ステップS 278)。セキュリティチップ5のMPU 51はステップS 265で復号されたソフトウェアを携帯電話機エンジン部110のROM15にインストールする(ステップS 2710)。そして、MPU 51はインストールが完了したことを示す信号を中央サーバ2へ送信する(ステップS 2711)。

#### 【0100】

一方、生体認証、電子証明書認証(PKI認証)、および環境認証の内、1つでも不適正フラグがセットされている場合(ステップS 275でNO)は、不適正フラグをセットする(ステップS 279)。この場合MPU 51はインストールを拒否することを示す信号を中央サーバ2へ送信する(ステップS 2712)。

#### 【0101】

ステップS 233でNOの場合、つまり携帯電話機1の主電源がオフの場合、中央サーバ2のCPU 21は記憶部25に記憶した提供用のソフトウェアを記憶部25から読み出す(ステップS 281)。CPU 21は、読み出したソフトウェアに、記憶部25に記憶したハッシュ関数を用いてメッセージダイジェストを算出する(ステップS 282)。CPU 21は認証機関サーバ3から予め発行を受けた中央サーバ2の個人鍵を個人鍵ファイル254から読み出し、ソフトウェア及びメッセージダイジェストを暗号化する(ステップS 283)。CPU 21は電子証明書ファイル253から認証機関サーバ3において予め発行を受けた電子証明書を読み出し、暗号化したソフトウェア及びメッセージダイジェストに電子証明書を添付して、FM放送局のコンピュータ(図示せず)へ送信する(ステップS 284)。

#### 【0102】

FM放送局のコンピュータは電子証明書、暗号化されたソフトウェア及びメッセージダイジェストをDARC規格の放送データに変換し、FM文字放送多重回路(図示せず)によってFM音楽データと放送データとに多重化する。これらのデータはFM変調発振器によりFM変調されて放送される。携帯電話機1は副ア

ンテナ部 117 から FM 文字放送を受信し（ステップ S 285）、DARC 規格の文字コードで記述されたデータを変換して電子証明書、暗号化したソフトウェア及びメッセージダイジェストを取り出す。なお、DARC 規格を利用した FM 文字放送に関する技術は特開平 10-116237 号に開示されている。

#### 【0103】

変換された、電子証明書、ソフトウェア及びメッセージダイジェストは第 2 ROM 116 に記憶される（ステップ S 286）。そして顧客の入力部 13 の操作により、主電源部 114 による電力の供給が開始された場合（ステップ S 291）、ステップ S 236～ステップ S 244 で説明した処理と同様に指紋認証を行い（ステップ S 292）、ステップ S 245～ステップ S 256 で説明した処理と同様に環境認証を行い（ステップ S 294）、ステップ S 262～ステップ S 274 で説明した処理と同様に電子証明書による認証を行う（ステップ S 293）。なお、電子証明書による認証を行う場合は、CPU 51 が第 2 ROM 116 に記憶された電子証明書、暗号化されたソフトウェア及びメッセージダイジェストを読み出して、RAM 52 に記憶してから、電子証明書による認証を行う。つまり、認証機関サーバ 3 から取得した公開鍵を用いて、電子証明書から公開鍵を取得し、取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する。

#### 【0104】

MPU 51 は ROM 55 に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てがアンド条件でセットされているか否かを判断する（ステップ S 295）。全ての適正フラグがセットされている場合（ステップ S 295 で YES）、送信されたソフトウェアを安全なものと判断し安全フラグをセットする（ステップ S 296）。セキュリティチップ 5 の MPU 51 は復号されたソフトウェアを携帯電話機エンジン部 110 の ROM 15 にインストールする（ステップ S 298）。そして、MPU 51 はインストールが完了したことを示す信号を中央サーバ 2 へ送信する（ステップ S 299）。

#### 【0105】

一方、生体認証、電子証明書認証（PKI 認証）、および環境認証の内、1つでも不適正フラグがセットされている場合（ステップS295でNO）は、不適正フラグをセットする（ステップS297）。この場合MPU51はインストールを拒否することを示す信号を中央サーバ2へ送信する（ステップS2910）。

#### 【0106】

中央サーバ2から提供されるソフトウェアはパッチ用ソフトウェア等の他、DDoS攻撃の対象となった携帯電話機1内のソフトウェアを削除するためのソフトウェアであっても良い。例えば、何らかの原因により、携帯電話機1に数日後に所定のWebサーバにDDoS攻撃を行うソフトウェア（プログラム）がセットされた場合、本発明の認証を経たソフトウェアを提供する。提供されるソフトウェアには、日時情報が記憶されており、インストールして実行することにより記憶された日時以降に記憶されたデータを全て消去する。

#### 【0107】

図30はインストールされた消去用ソフトウェアの処理内容を示すフローチャートである。ステップS298によりROM15に消去用のソフトウェアがインストールされる。顧客は消去用のソフトウェアを、入力部13を操作することによりCPU11に実行させる（ステップS301）。CPU11はROM15内の記憶履歴の読み出しを行う（ステップS302）。具体的には記憶されたファイル、インストールされたソフトウェア等のデータと、さらにそれらのデータが記憶された日時の情報を読み出す。CPU11は消去用のソフトウェアの実行プログラムから日時の情報を読み出す（ステップS303）。そして読み出した記憶履歴を参照し、読み出した日時以降に記憶されたデータを全て消去する（ステップS304）。これにより、DDoS攻撃の踏み台にされた携帯電話機1が、攻撃に利用されることを防止することができる。

#### 【0108】

##### 実施の形態5

図31は実施の形態5に係る携帯電話機1のハードウェア構成を示すブロック図である。実施の形態4に係る携帯電話機1を実行させるためのコンピュータブ

プログラムは、本実施の形態5のように携帯電話機1にプレインストールして提供することも、またCD-ROM、MO、メモリーカード等の可搬型記録媒体で提供することも可能である。さらに、コンピュータプログラムを回線経由で搬送波として伝搬させて提供することも可能である。すなわち、セキュリティチップ5を搭載する代わりに、セキュリティチップ5と同様の機能をもつコンピュータプログラムを携帯電話機1のROM17にインストールするようにしても良い。以下に、その内容を説明する。

#### 【0109】

図31に示す携帯電話機1に、生体情報を認証させ、環境情報を収集させ、環境情報を送信させ、電子証明書による認証をさせ、インストールさせるプログラムが記録された記録媒体1a（CD-ROM、MO、メモリーカード又はDVD-ROM等）が携帯電話機1のROM15にインストールされている。インストールの方法としては、外部接続端子19に接続可能なメモリーカード等の記録媒体1aを嵌挿し、プログラムをインストールするか、または、中央サーバ2から本発明に係るプログラムをダウンロードするようにしても良い。係るプログラムは携帯電話機1のRAM12にロードして実行される。これにより、上述のような本発明の情報処理装置としての携帯電話機1として機能する。

#### 【0110】

##### 実施の形態6

本実施の形態においては、携帯電話機1及び中央サーバ2の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機1及び中央サーバ2を安全と判断しその後の情報の送受信を許可する技術について説明する。

#### 【0111】

図32は実施の形態6に係る携帯電話機1のハードウェア構成を示すブロック図であり、また図33は実施の形態6に係る中央サーバ2のハードウェア構成を示すブロック図である。図32に示すように本実施の形態においては携帯電話機1においても中央サーバ2の環境認証を行うため、携帯電話機1のROM15には環境情報DB151が用意されている。図4で説明したものと同様に、中央サ

ーバ2の外部通信ポート29に接続される周辺機器、PCカード（図示せず）、インストールされているOS、ソフトウェア等に対する環境情報に対する条件が、セキュリティポリシーである階級に対応付けられて記憶されている。

#### 【0112】

中央サーバ2も携帯電話機1による認証を受けるべく、指紋取得部212及びセキュリティチップ5がバス27を介してCPU21に接続されている。なお、これらの詳細については既に実施の形態1で説明したとおりであるので詳細な説明は省略する。また29はUSBポート、RS232Cポート等の外部通信ポートであり、プリンタ、マウス、ハードディスク、MO等の周辺機器が接続される。

#### 【0113】

本実施の形態においては、携帯電話機1及び中央サーバ2の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機1及び中央サーバ2を安全と判断しその後の情報の送受信を許可するために、図11に示すステップS115以降に、すなわち携帯電話機1の安全性が確認された後に、以下の処理を追加して行う。

#### 【0114】

図34乃至図37は実施の形態6に係る認証処理の手順を示すフローチャートである。ステップS115の後、中央サーバ2のセキュリティチップ5のMPU51は制御プログラム55Pを実行し、表示部24に指紋情報の取得要求を表示する（ステップS341）。指紋取得部212から指紋情報が入力された場合、セキュリティチップ5のMPU51は指紋情報を受け付け（ステップS342）、RAM52に一時的に記憶する。そして、MPU51はROM55の指紋情報ファイル552に携帯電話機1の購入時に予め記憶してある指紋情報を読み出し、RAM52に記憶した指紋情報と比較して一致するか否か、すなわち指紋情報認証が適正であるか否か判断する（ステップS343）。

#### 【0115】

指紋が一致し、指紋情報認証が適正であると判断した場合は（ステップS343でYES）、指紋認証適正フラグをセットし、セットした指紋認証適正フラグ

を携帯電話機 1 へ送信する（ステップ S 3 4 5）。一方、指紋が一致せず、指紋情報認証が不適正であると判断した場合（ステップ S 3 4 3 で NO）、指紋認証不適正フラグセットし、セットした指紋認証不適正フラグを携帯電話機 1 へ送信する（ステップ S 3 4 4）。携帯電話機 1 の CPU 11 は送信された指紋認証フラグ（指紋認証適正フラグまたは指紋認証不適正フラグ）を ROM 15 に記憶する（ステップ S 3 4 6）。なお、本実施の形態においては指紋を用いた生体認証を中央サーバ 2 において実行することとしたが、予め採取した指紋情報を認証機関サーバ 3 または携帯電話機 1 に記憶しておき、認証機関サーバ 3 または携帯電話機 1 において判断するようにしても良い。これにより指紋を用いた生体認証が終了する。

#### 【0116】

続いて、セキュリティチップ 5 の MPU 5 1 は中央サーバ 2 の環境情報を取得する（ステップ S 3 4 7）。環境情報の収集は、上述したように MPU 5 1 が中央サーバ 2 の ROM 15 の OS、BIOS 及びインストールされるソフトウェアを常駐して監視し、中央サーバ 2 の機器名、OS の名称、バージョン、外部通信ポート 2 9 に接続された周辺機器の機器名、バージョン、インストールされたブラウザ等のソフトウェアのソフト名、バージョンなどを収集することにより行われる。収集された環境情報は環境情報ファイル 5 5 1 に記憶される（ステップ S 3 4 8）。

#### 【0117】

セキュリティチップ 5 の MPU 5 1 は RAM 5 2 に記憶した環境情報ファイル 5 5 1 に記憶した環境情報を読み出す（ステップ S 3 4 9）。セキュリティチップ 5 の MPU 5 1 は、読み出した環境情報に、ROM 5 5 に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップ S 3 5 1）。MPU 5 1 は認証機関サーバ 3 から予め発行を受けた中央サーバ 2 の個人鍵を個人鍵ファイル 5 5 4 から読み出し、環境情報及びメッセージダイジェストを暗号化する（ステップ S 3 5 2）。さらに、MPU 5 1 は電子証明書ファイル 5 5 3 から認証機関サーバ 3 において予め発行を受けた電子証明書を読み出し、暗号化した環境情報及びメッセージダイジェストに電子証明書を添付して携帯電話機 1 へ送信す

る（ステップS353）。携帯電話機1のCPU11は送信された電子証明書、暗号化された環境情報及びメッセージダイジェストをRAM12に記憶する。

#### 【0118】

携帯電話機1のCPU11は電子証明書に記載されている認証機関サーバ3へアクセスし、受信した電子証明書の公開鍵（認証機関の公開鍵）の取得を要求する（ステップS354）。認証機関サーバ3は、電子証明書の公開鍵を携帯電話機1へ送信し、携帯電話機1は送信された電子証明書の公開鍵を受信する（ステップS355）。携帯電話機1のCPU11は、記憶した電子証明書をRAM12から読み出し、認証機関サーバ3から送信された認証機関の公開鍵を用いて電子証明書を復号し中央サーバ2の公開鍵を取得する（ステップS356）。

#### 【0119】

携帯電話機1のCPU11は取得した中央サーバ2の公開鍵を用いて暗号化された環境情報及びメッセージダイジェストを復号する（ステップS361）。さらにCPU11は復号した環境情報に、携帯電話機1のROM55に記憶したハッシュ関数を用いてメッセージダイジェストを算出する（ステップS362）。携帯電話機1のCPU11はステップS361で復号したメッセージダイジェストと、ステップS362で算出したメッセージダイジェストとが一致するか否か、すなわち送信の途中で注文情報に改竄がないか、また権限のある中央サーバ2から情報が送受信されたものであるか否かを判断する（ステップS363）。

#### 【0120】

メッセージダイジェストが一致しない場合は（ステップS363でNO）、CPU11は何らかの改竄またはなりすましがあったと判断し、電子証明書認証の不適正フラグをセットする（ステップS365）。一方、メッセージダイジェストが一致する場合は（ステップS363でYES）、なりすまし及び改竄がないものとして電子証明書の適正フラグをセットする（ステップS364）。そして、携帯電話機1のCPU11は電子証明書認証のフラグ（電子証明書認証適正フラグ、または電子証明書認証不適正フラグ）をROM15に記憶する（ステップS366）。

#### 【0121】



携帯電話機 1 の CPU 11 はステップ S 104 で決定した階級に対応する環境情報の条件を環境情報 DB 151 から読み出す (ステップ S 371)。そして、CPU 11 は、復号された環境情報が、ステップ S 371 にて読み出された環境情報の条件を満たすか否かを判断する (ステップ S 372)。条件を満たさない場合 (ステップ S 372 で NO)、環境認証不適正フラグをセットする (ステップ S 374)。一方、条件を満たす場合 (ステップ S 372 で YES)、環境認証適正フラグをセットする (ステップ S 373)。携帯電話機 1 の CPU 11 は環境認証のフラグ (環境認証適正フラグ、または環境認証不適正フラグ) を ROM 15 に記憶する (ステップ S 375)。

#### 【0122】

CPU 11 は、ROM 15 に記憶した指紋認証フラグ、電子証明書フラグ及び環境認証フラグを読み出し、指紋認証適正フラグ、電子証明書適正フラグ及び環境認証適正フラグの全てが AND 条件でセットされているか否かを判断する (ステップ S 376)。全ての適正フラグがセットされている場合 (ステップ S 376 で YES)、中央サーバ 2 を安全なものとして判断し安全フラグをセットし、ステップ S 121 へ移行する (ステップ S 377)。

#### 【0123】

一方、生体認証、電子証明書認証 (PKI 認証)、および環境認証の内、1 つでも不適正フラグがセットされている場合 (ステップ S 376 で NO) は、不適正フラグをセットし、ステップ S 123 へ移行する (ステップ S 378)。このように、携帯電話機 1 及び中央サーバ 2 の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に限り、携帯電話機 1 及び中央サーバ 2 を安全と判断しその後の情報の送受信を許可するようにしたので、より安全性の高い通信環境を提供することが可能となる。

#### 【0124】

なお、本実施の形態においては、携帯電話機 1 及び中央サーバ 2 の双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機 1 及び中央サーバ 2 を安全と判断しその後の情報の送受信を許可する技術について説明したが、同様に携帯電話機 1 及びオンラインショップの Web サー

バ4間（または図示しない他の携帯電話機、洗濯機、パーソナルコンピュータ等の情報処理装置）についても、双方で生体情報認証、環境認証及び電子証明書認証の全てが適正と判断された場合に、携帯電話機1及びWebサーバ4等を安全と判断しその後の情報の送受信を許可するようにしても良いことは言うまでもない。

#### 【0125】

実施の形態2乃至6は以上の如き構成としてあり、その他の構成及び作用は実施の形態1と同様であるので、対応する部分には同一の参照番号を付してその詳細な説明を省略する。

（付記1） 情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、  
受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第1認証装置または第2認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第1認証装置へ送信する環境情報送信ステップと、

予め前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記情報処理装置から前記第1認証装置へ送信する暗号化情報送信ステップと、

前記第1認証装置により、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記第1認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステッ

プによる認証が全て適正である場合に前記第 1 認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

(付記 2) 情報処理装置、第 1 認証装置及び第 2 認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第 1 認証装置または第 2 認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を前記情報処理装置から前記第 1 認証装置へ送信する環境情報送信ステップと、

前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記第 1 認証装置から前記情報処理装置へ送信する暗号化情報送信ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記第 1 認証装置により、前記送信された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記情報処理装置により、前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記復号したソフトウェアを前記情報処理装置にインストールするインストールステップと

を備えることを特徴とする安全性判断方法。

(付記 3) 情報処理装置、第 1 認証装置及び第 2 認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断方法において

て、

前記情報処理装置により、生体情報を受け付ける生体情報受付ステップと、  
受け付けた生体情報が適正であるか否かを前記情報処理装置、前記第1認証装置または第2認証装置により判断する生体情報認証ステップと、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集ステップと、

収集した環境情報を、前記第2認証装置から発行を受けた個人鍵で暗号化する暗号化ステップと、

予め前記第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された環境情報を前記情報処理装置から前記第1認証装置へ送信する暗号化情報送信ステップと、

前記第1認証装置により、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する電子証明書認証ステップと、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記第1認証装置により、前記復号された環境情報が適正であるか否かを判断する環境情報認証ステップと、

前記生体情報認証ステップ、環境情報認証ステップ及び電子証明書認証ステップによる認証が全て適正である場合に前記第1認証装置により、前記情報処理装置を安全と判断する安全判断ステップと

を備えることを特徴とする安全性判断方法。

(付記4) 情報処理装置、第1認証装置及び第2認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第 1 認証装置へ送信する環境情報送信手段と、  
前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第 1 認証装置へ送信する暗号化情報送信手段とを備え、  
前記第 1 認証装置は、  
前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、  
送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、  
前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と  
を備えることを特徴とする安全性判断システム。

(付記 5) 前記環境情報送信手段及び暗号化情報送信手段は、収集した環境情報を前記個人鍵で暗号化して、前記電子証明書と共に前記第 1 認証装置へ送信するよう構成してあることを特徴とする付記 4 に記載の安全性判断システム。

(付記 6) 前記情報処理装置との間で商取引に関する情報を送受信する店舗コンピュータをさらに備え、

前記情報処理装置は、商品情報または金額情報を含む商取引に関する情報を受け付ける手段をさらに備え、

前記暗号化情報送信手段は、前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化された前記商取引に関する情報を前記第 1 認証装置へ送信するよう構成してあり、

前記環境情報認証手段は、送信された商品情報または金額情報に対応する階級に係る環境条件を環境情報データベースから読み出し、該読み出した環境条件に前記送信された環境情報が合致するか否かにより、適正であるか否かを判断するよう構成してあり、

前記第 1 認証装置は、前記安全判断手段により前記情報処理装置が安全と判断した場合に、該情報処理装置の安全性に関する情報を前記店舗コンピュータへ送

信する手段をさらに備えることを特徴とする付記 4 に記載の安全性判断システム

（付記 7） 前記第 1 認証装置は、  
生体情報を受け付ける副生体情報受付手段と、  
受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、  
接続された周辺機器またはインストールされたソフトウェアの情報を含む環境  
情報を収集する副環境情報収集手段と、

前記第 2 認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収  
集した環境情報を暗号化する副暗号化手段と、

前記第 2 認証装置から発行を受けた電子証明書及び前記暗号化された環境情報  
を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、

前記情報処理装置は、

前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から  
取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正  
であるか否かを判断する副電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報デー  
タベース及び復号された環境情報を参照して、前記送信された環境情報が適正で  
あるか否かを判断する副環境情報認証手段と、

前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段によ  
る認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に  
、前記情報処理装置及び前記第 1 認証装置を安全と判断する副安全判断手段と  
を備えることを特徴とする付記 4 に記載の安全性判断システム。

（付記 8） 情報処理装置、第 1 認証装置及び第 2 認証装置が通信網を介し  
て接続されており、前記情報処理装置の安全性を判断する安全性判断システムに  
おいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境

情報を収集する環境情報収集手段と、

収集した環境情報を前記第 1 認証装置へ送信する環境情報送信手段とを備え、

前記第 1 認証装置は、

前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを前記情報処理装置へ送信する暗号化情報送信手段とを備え、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベースを参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記情報処理装置は、

前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記復号したソフトウェアをインストールするインストール手段とをさらに備える

ことを特徴とする安全性判断システム。

(付記 9) 前記情報処理装置は、主電力供給手段と、副電力供給手段と、副電力供給手段から電力の供給をうける受信用通信手段と、前記主電力供給手段による電力の供給が行われていない場合に、前記暗号化情報送信手段により送信された電子証明書及び個人鍵で暗号化されたソフトウェアを前記受信用通信手段により受信して蓄積する蓄積手段とをさらに備えることを特徴とする付記 8 に記載の安全性判断システム。

(付記 10) 前記電子証明書認証手段は、前記主電力供給手段による電力の供給が行われた場合に、前記蓄積手段により蓄積した電子証明書及びソフトウェアを読み出し、前記第 2 認証装置から取得した公開鍵を用いて、前記電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断するよう構成してあることを特徴とする付記 9 に記載の安全判断システム。

(付記 11) 前記ソフトウェアは、前記情報処理装置に予めインストール

されているソフトウェアのパッチ用ソフトウェアであることを特徴とする付記 8 乃至 10 に記載の安全判断システム。

(付記 12) 前記情報処理装置は、前記インストール手段によりインストールしたソフトウェアを実行した場合、所定の日時以降に記憶部に記憶されたデータを消去する消去手段をさらに備えることを特徴とする付記 8 乃至 10 に記載の安全判断システム。

(付記 13) 情報処理装置、第 1 認証装置及び第 2 認証装置が通信網を介して接続されており、前記情報処理装置の安全性を判断する安全性判断システムにおいて、

前記情報処理装置は、

生体情報を受け付ける生体情報受付手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

前記第 2 認証装置から発行を受けた個人鍵で前記生体情報受付手段により受け付けた生体情報及び前記環境情報収集手段により収集した環境情報を暗号化する暗号化手段と、

前記第 2 認証装置から発行を受けた電子証明書及び前記暗号化された生体情報及び環境情報を前記第 1 認証装置へ送信する暗号化情報送信手段とを備え、

前記第 1 認証装置は、

前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された生体情報及び環境情報を復号し、復号された生体情報及び環境情報が適正であるか否かを判断する電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する環境情報認証手段と、

前記復号された生体情報と、予め記憶された生体情報とを比較して適正であるか否かを判断する生体情報認証手段と、

前記生体情報認証手段、環境情報認証手段及び電子証明書認証手段による認証が全て適正である場合に前記情報処理装置を安全と判断する安全判断手段と



を備えることを特徴とする安全性判断システム。

(付記 14) 前記環境情報は、インストールされたソフトウェアの名称またはバージョン、接続された周辺機器の機器名またはバージョン、または、前記情報処理装置の装置名またはバージョンの情報を含むことを特徴とする付記 4 乃至 13 のいずれかに記載の安全判断システム。

(付記 15) 前記生体情報は、音声、指紋、網膜、または虹彩の情報であることを特徴とする付記 4 乃至 14 のいずれかに記載の安全判断システム。

(付記 16) 第 1 認証装置及び第 2 認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第 1 認証装置へ送信する環境情報送信手段と、

前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第 1 認証装置へ送信する暗号化情報送信手段と、

前記生体情報認証手段により適正と判断され、また前記環境情報送信手段により送信した環境情報が前記第 1 認証手段により適正と判断され、かつ、前記暗号化情報送信手段により送信した電子証明書及び暗号化された情報が前記第 1 認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする安全性判断装置。

(付記 17) 第 1 認証装置及び第 2 認証装置に通信網を介して接続される情報処理装置の安全性を判断する安全性判断装置において、

受け付けた生体情報が適正であるか否かを判断する生体情報認証手段と、

前記情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する環境情報収集手段と、

収集した環境情報を前記第 1 認証装置へ送信する環境情報送信手段と、

前記第 1 認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第 2 認証装置から取得した公開鍵を用いて電子証明書から取得した公開

鍵で、暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する電子証明書認証手段と、

前記生体情報認証手段及び電子証明書認証手段による認証が適正であると判断され、また前記環境情報送信手段により送信した環境情報が前記第1認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記情報処理装置に前記復号したソフトウェアをインストールするインストール手段と

を備えることを特徴とする安全性判断装置。

(付記18) 通信網を介して接続される情報処理装置の安全性を判断する第1認証装置において、

前記情報処理装置により受け付けた生体情報が適正であるか否かの認証情報を受信する認証情報受信手段と、

通信網を介して接続された第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報が、前記情報処理装置から送信された場合に、前記第2認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する電子証明書認証手段と、

前記情報処理装置から、該情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を受信した場合に、送受信される情報に応じて階級付けされた環境条件を記憶した環境情報データベース及び送信された情報を参照して、受信した環境情報が適正であるか否かを判断する環境情報認証手段と、

前記認証情報受信手段により、生体情報が適正であるとの認証情報を受信し、また前記環境情報認証手段及び電子証明書認証手段による認証が適正であると判断した場合に前記情報処理装置を安全と判断する安全判断手段と

を備えることを特徴とする第1認証装置。

(付記19) 第1認証装置及び第2認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第 1 認証装置へ送信させる環境情報送信ステップと、

コンピュータに、前記第 2 認証装置から発行を受けた電子証明書及び個人鍵で暗号化された情報を前記第 1 認証装置へ送信させる暗号化情報送信ステップと、

コンピュータに、前記生体情報認証ステップにより適正と判断され、また前記環境情報送信ステップにより送信された環境情報が前記第 1 認証装置により適正と判断され、かつ、前記暗号化情報送信ステップにより送信された電子証明書及び暗号化された情報が前記第 1 認証装置により適正と判断され、前記第 1 認証装置から適正であることを示す情報を受信した場合に、コンピュータを安全と判断する安全判断ステップと

を実行させることを特徴とするコンピュータプログラム。

(付記 20) 第 1 認証装置及び第 2 認証装置に通信網を介して接続されるコンピュータの安全性を判断するためのコンピュータプログラムにおいて、

コンピュータに、受け付けた生体情報が適正であるか否かを認証させる生体情報認証ステップと、

コンピュータに、接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集させる環境情報収集ステップと、

コンピュータに、収集させた環境情報を前記第 1 認証装置へ送信させる環境情報送信ステップと、

コンピュータに、前記第 1 認証装置から電子証明書及び暗号化されたソフトウェアを受信した場合、前記第 2 認証装置から取得した公開鍵を用いて、電子証明書から取得した公開鍵で暗号化されたソフトウェアを復号させ、復号されたソフトウェアが適正であるか否かを判断させる電子証明書認証ステップと、

コンピュータに、前記生体情報認証ステップ及び電子証明書認証ステップによる認証が適正であると判断し、また、前記環境情報送信ステップにより送信した環境情報が前記第 1 認証装置により適正と判断され、適正であることを示す情報を受信した場合に、前記コンピュータに前記復号したソフトウェアをインストー

ルするインストールステップと

を実行させることを特徴とするコンピュータプログラム。

(付記 2 1) 前記第 1 認証装置により、生体情報を受け付ける副生体情報受付ステップと、

受け付けた生体情報が適正であるか否かを前記情報処理装置、第 1 認証装置または第 2 認証装置により判断する副生体情報認証ステップと、

前記第 1 認証装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集ステップと、

前記第 2 認証装置から発行を受けた個人鍵で前記副環境情報収集ステップにより収集した環境情報を暗号化する副暗号化ステップと、

前記第 2 認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信ステップと、

前記情報処理装置により、前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証ステップと

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記情報処理装置により前記送信された環境情報が適正であるか否かを判断する副環境情報認証ステップと、

前記副生体情報認証ステップ、副環境情報認証ステップ及び副電子証明書認証ステップによる認証が全て適正であり、かつ前記安全判断ステップにより安全と判断された場合に、前記情報処理装置及び前記第 1 認証装置を安全と判断する副安全判断ステップと

を備えることを特徴とする付記 1 または 3 に記載の安全性判断方法。

(付記 2 2) 前記第 1 認証装置は、

生体情報を受け付ける副生体情報受付手段と、

受け付けた生体情報が適正であるか否かを判断する副生体情報認証手段と、

接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する副環境情報収集手段と、

前記第 2 認証装置から発行を受けた個人鍵で前記副環境情報収集手段により収集した環境情報を暗号化する副暗号化手段と、

前記第 2 認証装置から発行を受けた電子証明書及び前記暗号化された環境情報を前記情報処理装置へ送信する副暗号化情報送信手段とを備え、

前記情報処理装置は、

前記第 2 認証装置から取得した公開鍵を用いて前記送信された電子証明書から取得した公開鍵で、暗号化された環境情報を復号し、復号された環境情報が適正であるか否かを判断する副電子証明書認証手段と、

送受信される情報に応じて階級付けされた環境条件を記憶した副環境情報データベース及び復号された環境情報を参照して、前記送信された環境情報が適正であるか否かを判断する副環境情報認証手段と、

前記副生体情報認証手段、副環境情報認証手段及び副電子証明書認証手段による認証が全て適正であり、かつ前記安全判断手段により安全と判断された場合に、前記情報処理装置及び前記第 1 認証装置を安全と判断する副安全判断手段とを備えることを特徴とする付記 12 に記載の安全判断システム。

#### 【0126】

##### 【発明の効果】

以上詳述した如く、本発明にあつては、利用者の指紋等の生体情報を受け付け、受け付けた生体情報が適正であるか否かを判断する。また、情報処理装置に接続された周辺機器またはインストールされたソフトウェアの情報を含む環境情報を収集する。情報処理装置は収集した環境情報を第 1 認証装置へ送信する。さらに、第 2 認証装置から発行を受けた電子証明書及び情報処理装置の個人鍵で暗号化された商取引に関する情報等を第 1 認証装置へ送信する。第 1 認証装置は、電子証明書及び暗号化された情報を受信した場合、第 2 認証装置から取得した第 2 認証装置（認証機関）の公開鍵を用いて、送信された電子証明書から情報処理装置の公開鍵を取得する。そして、取得した情報処理装置の公開鍵で暗号化された情報を復号し、復号された情報が適正であるか否かを判断する。

#### 【0127】

第 1 認証装置は、送受信される情報に応じて階級付けされた環境情報の条件を

記憶した環境情報データベース及び送信された情報を参照して、送信された環境情報が適正であるか否かを判断する。そして、生体情報認証、環境情報認証、及び電子証明書認証による認証が全て適正である場合に情報処理装置を安全と判断する。このように構成したので、情報処理装置の安全性を確保しつつ、円滑な情報の送受信及び商取引を実現することが可能となる。さらに、第1認証装置においても生体情報認証、電子証明書認証及び環境認証をおこない、情報処理装置における生体情報認証、電子証明書認証及び環境認証、並びに、第1に認証装置における生体情報認証、電子証明書認証及び環境認証において、全て適正と判断された場合のみ、第1認証装置及び情報処理装置の双方を安全と判断するようにしたので、さらに高度な安全性を確保することが可能となる。

#### 【0128】

また、本発明にあつては、利用者の生体情報を受け付け、受け付けた生体情報が適正であるか否かの本人認証を行う。そして情報処理装置は収集した環境情報を第1認証装置へ送信し、第1認証装置において、環境情報の認証を行う。第1認証装置から情報処理装置へパッチ用のソフトウェア等を送信する場合は、第1認証装置は、第2認証装置から発行を受けた電子証明書及び個人鍵で暗号化されたソフトウェアを情報処理装置へ送信する。情報処理装置は、電子証明書及び暗号化されたソフトウェアを受信した場合、第2認証装置へ公開鍵を要求し、この認証機関の公開鍵を用いて電子証明書から第1認証装置の公開鍵を取得する。そしてこの公開鍵で暗号化されたソフトウェアを復号し、復号されたソフトウェアが適正であるか否かを判断する。最後に、上述した本人認証、環境認証及び電子証明書による認証が全て適正であると判断した場合、復号したソフトウェアを情報処理装置へインストールする。このように構成したので、第3者のなりすましを防止でき、高度な安全性を維持した上で情報処理装置へパッチ用のソフトウェア、ファームウェア等のソフトウェアを提供することが可能となる。

#### 【0129】

さらに、本発明にあつては、情報処理装置は、主電力供給手段及び副電力供給手段を備え、受信用通信手段は副電力供給手段から電力の供給をうける構成としている。主電力供給手段による電力の供給が行われていない場合、すなわちメイ

ンの電源がオンにされていない場合に、第1認証装置から電子証明書及び個人鍵で暗号化されたソフトウェアが送信された場合は、サブバッテリーを用いた受信用通信手段によりこれらの情報を受信して蓄積する。そして、主電力供給手段による電力の供給が行われた場合に、蓄積した電子証明書及びソフトウェアを読み出し、送信されたソフトウェアが適正であるか否かの判断、本人認証及び環境認証を行うようにしたので、電源をオンにしていない顧客に対してもパッチ用のソフトウェアを、安全性を確保した上で大量に配布することが可能となる。また特に提供するソフトウェアとして、所定の日時以降に記憶されたデータを記憶部から消去するソフトウェアを提供することによりDDoS攻撃の踏み台にされることを効果的に防止することが可能となる等、本発明は優れた効果を奏し得る。

【図面の簡単な説明】

【図1】

本発明に係る安全性判断システムの概要を示す模式図である。

【図2】

携帯電話機のハードウェア構成を示すブロック図である。

【図3】

中央サーバのハードウェア構成を示すブロック図である。

【図4】

環境情報DBのレコードレイアウトを示す説明図である。

【図5】

Webサーバと携帯電話機との間の商取引の手順を示すフローチャートである。

【図6】

Webページのイメージを示す説明図である。

【図7】

安全性の判断処理の手順を示すフローチャートである。

【図8】

安全性の判断処理の手順を示すフローチャートである。

【図9】

安全性の判断処理の手順を示すフローチャートである。

【図 10】

安全性の判断処理の手順を示すフローチャートである。

【図 11】

安全性の判断処理の手順を示すフローチャートである。

【図 12】

安全性の判断処理の手順を示すフローチャートである。

【図 13】

実施の形態 2 に係る携帯電話機のハードウェア構成を示すブロック図である。

【図 14】

実施の形態 3 に係る携帯電話機のハードウェア構成を示すブロック図である。

【図 15】

中央サーバのハードウェア構成を示すブロック図である。

【図 16】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャートである。

【図 17】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャートである。

【図 18】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャートである。

【図 19】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャートである。

【図 20】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャートである。

【図 21】

実施の形態 4 に係る携帯電話機のハードウェア構成を示すブロック図である。

【図 22】

中央サーバのハードウェア構成を示すブロック図である。

【図 23】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャートである。



## 【図 24】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャートである

## 【図 25】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャートである

## 【図 26】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャートである

## 【図 27】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャートである

## 【図 28】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャートである

## 【図 29】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャートである

## 【図 30】

インストールされた消去用ソフトウェアの処理内容を示すフローチャートである。

## 【図 31】

実施の形態 5 に係る携帯電話機のハードウェア構成を示すブロック図である。

## 【図 32】

実施の形態 6 に係る携帯電話機のハードウェア構成を示すブロック図である。

## 【図 33】

実施の形態 6 に係る中央サーバのハードウェア構成を示すブロック図である。

## 【図 34】

実施の形態 6 に係る認証処理の手順を示すフローチャートである。

【図 3 5】

実施の形態 6 に係る認証処理の手順を示すフローチャートである。

【図 3 6】

実施の形態 6 に係る認証処理の手順を示すフローチャートである。

【図 3 7】

実施の形態 6 に係る認証処理の手順を示すフローチャートである。

【符号の説明】

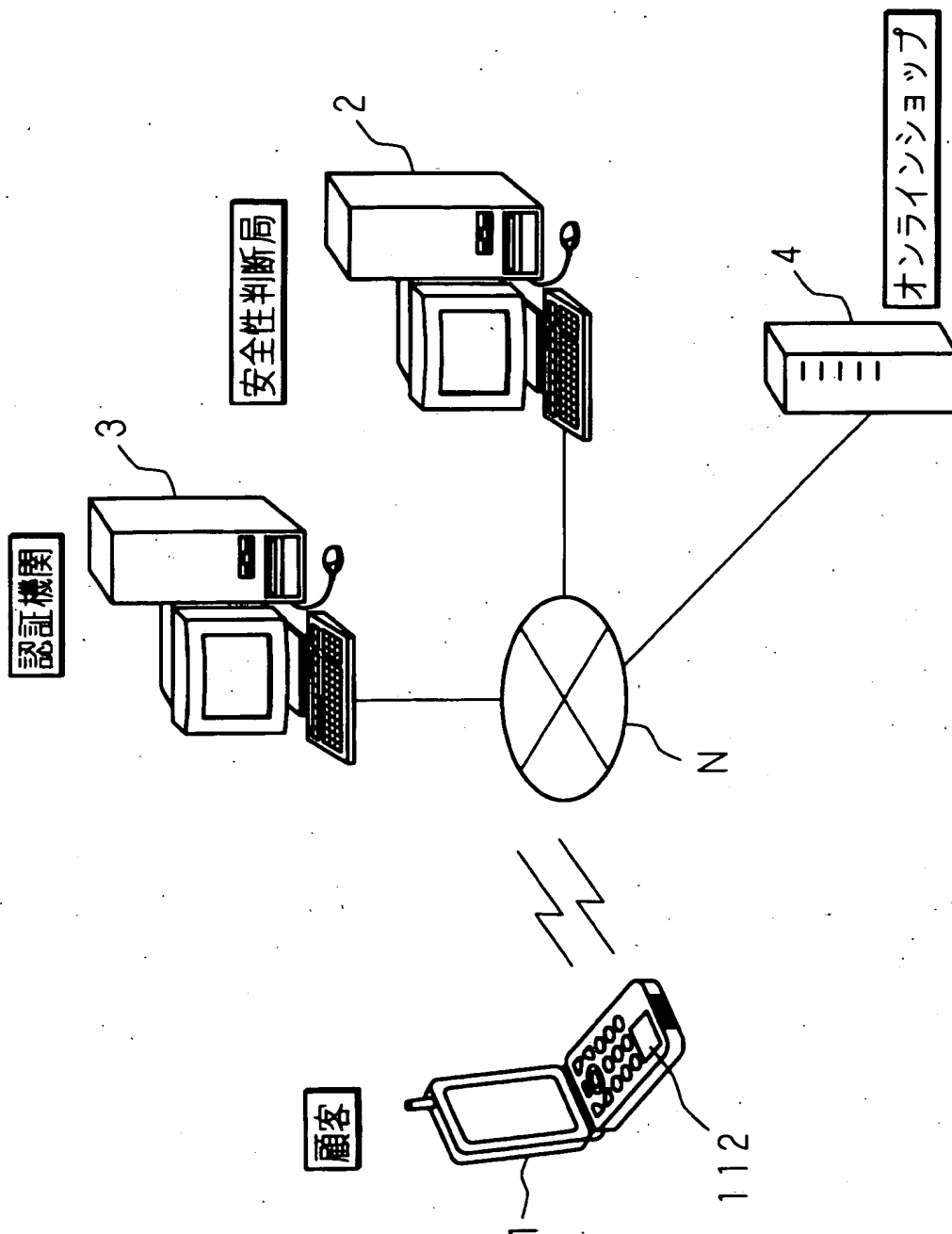
- 1 携帯電話機（情報処理装置）
- 1 1 2 指紋取得部
- 2 中央サーバ（第 1 認証装置）
- 3 認証機関サーバ（第 2 認証装置）
- 4 Webサーバ（店舗コンピュータ）
- N インターネット（通信網）
- 1 1 0 携帯電話機エンジン部
- 1 5 ROM
- 1 6 アンテナ部
- 1 3 入力部
- 1 1 3 電源部
- 1 9 外部接続端子
- 5 セキュリティチップ（安全性判断装置）
- 5 5 2 指紋情報ファイル
- 5 5 1 環境情報ファイル
- 5 5 3 電子証明書ファイル
- 5 5 4 個人鍵ファイル
- 2 4 表示部
- 2 3 入力部
- 2 5 1 環境情報データベース（環境情報 DB）
- 1 a 記録媒体

- 114 主電源部 (主電力供給手段)
- 115 副電源部 (副電力供給手段)
- 116 第2ROM (蓄積手段)

【書類名】 図面

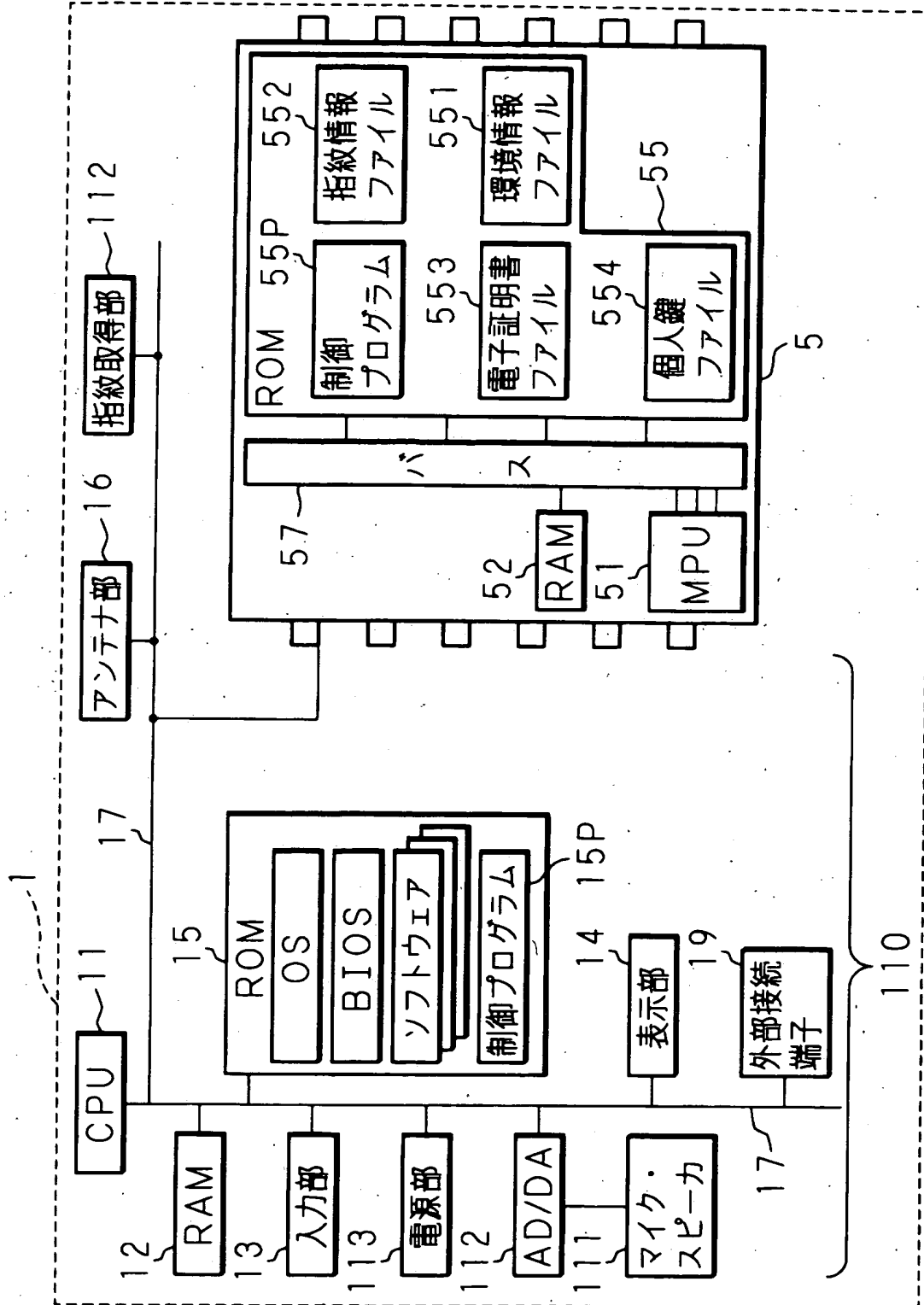
【図 1】

本発明に係る安全性判断システムの概要を示す模式図



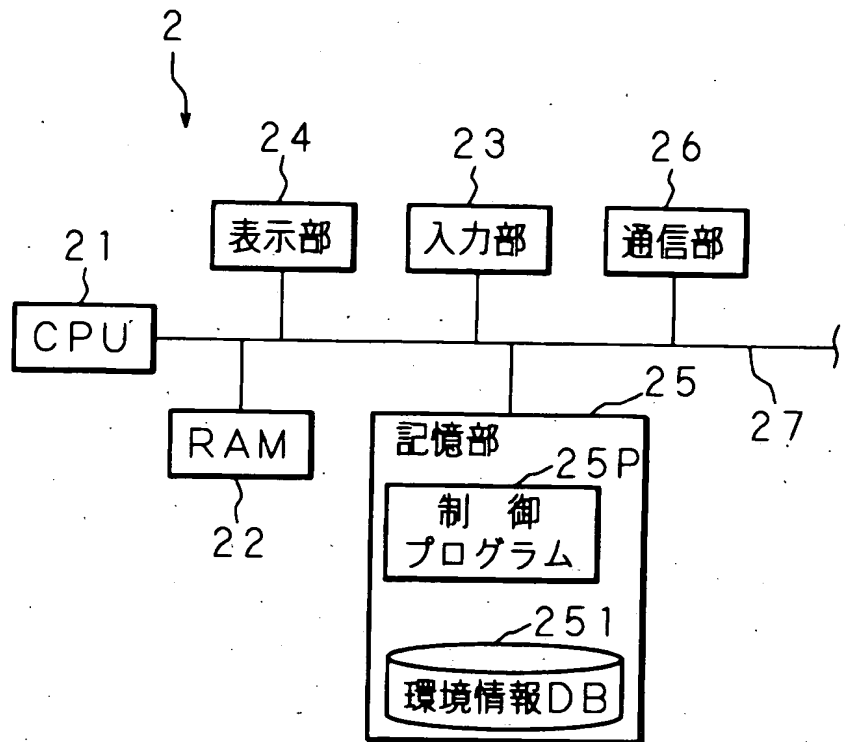
【図 2】

携帯電話機のハードウェア構成を示すブロック図



【図 3】

中央サーバのハードウェア構成を示すブロック図

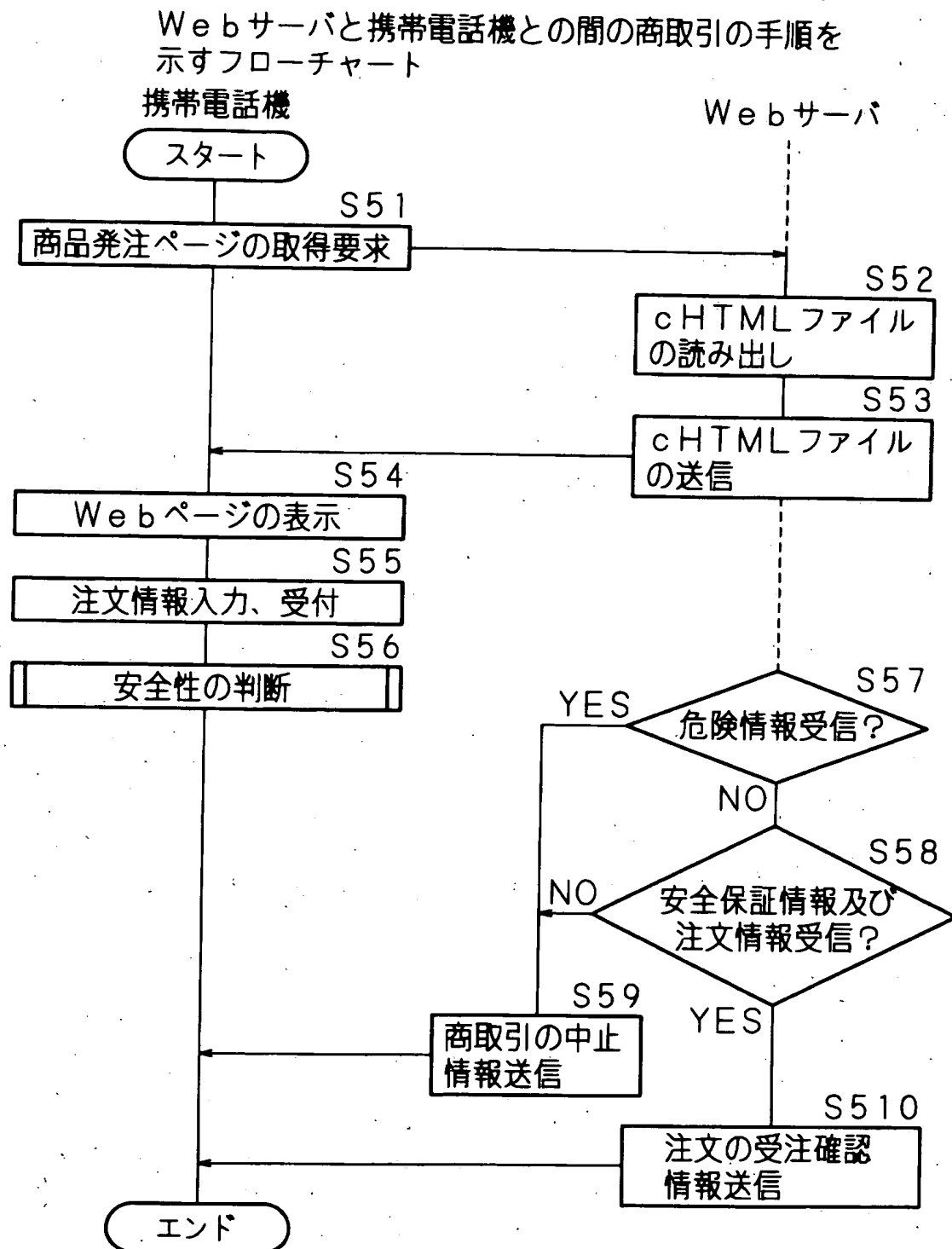


【図 4】

環境情報DBのレコードレイアウトを示す説明図

階級	金額情報	商品情報	環境条件					
			装置情報		ソフトウェア		周辺機器	
			装置名	バージョン	ソフト名	バージョン	機器名	バージョン
6	~100円	着メロ 画像データ ...	S001~ S004 F001~ F004 N001~ N004 ...	1.0以上 1.0以上 — : 1.5以上	A B C : B C : :	2.0以上 1.0以上 1.0以上 : 2.5以上 1.0以上 : :	XX XY ZZ : XX XY : :	1.0以上 2.0以上 3.0以上 : 2.0以上 2.0以上 : :
5	101円~ 3,000円	一般文書 ファイル ...	S003, S004 F003, F004 N003, N004 ...	1.5以上 — — : : :	B C : : C :	2.5以上 1.0以上 : : 3.0以上 :	XX XY : : — :	2.0以上 2.0以上 : : — :
1	50,000円~	株券 ...	S004 F004 N004 ...	2.0以上 — — : :	C : : :	3.0以上 : : :	— : : :	— : : :

【図 5】





【図 6】

## Web ページのイメージを示す説明図

商品発注メニュー

プリンタ

インクジェット ○××-△△ ▼

数量 1 ▼

スキャナ

△△△××× ▼

数量 0 ▼

...

合計金額 29,800円

発注する

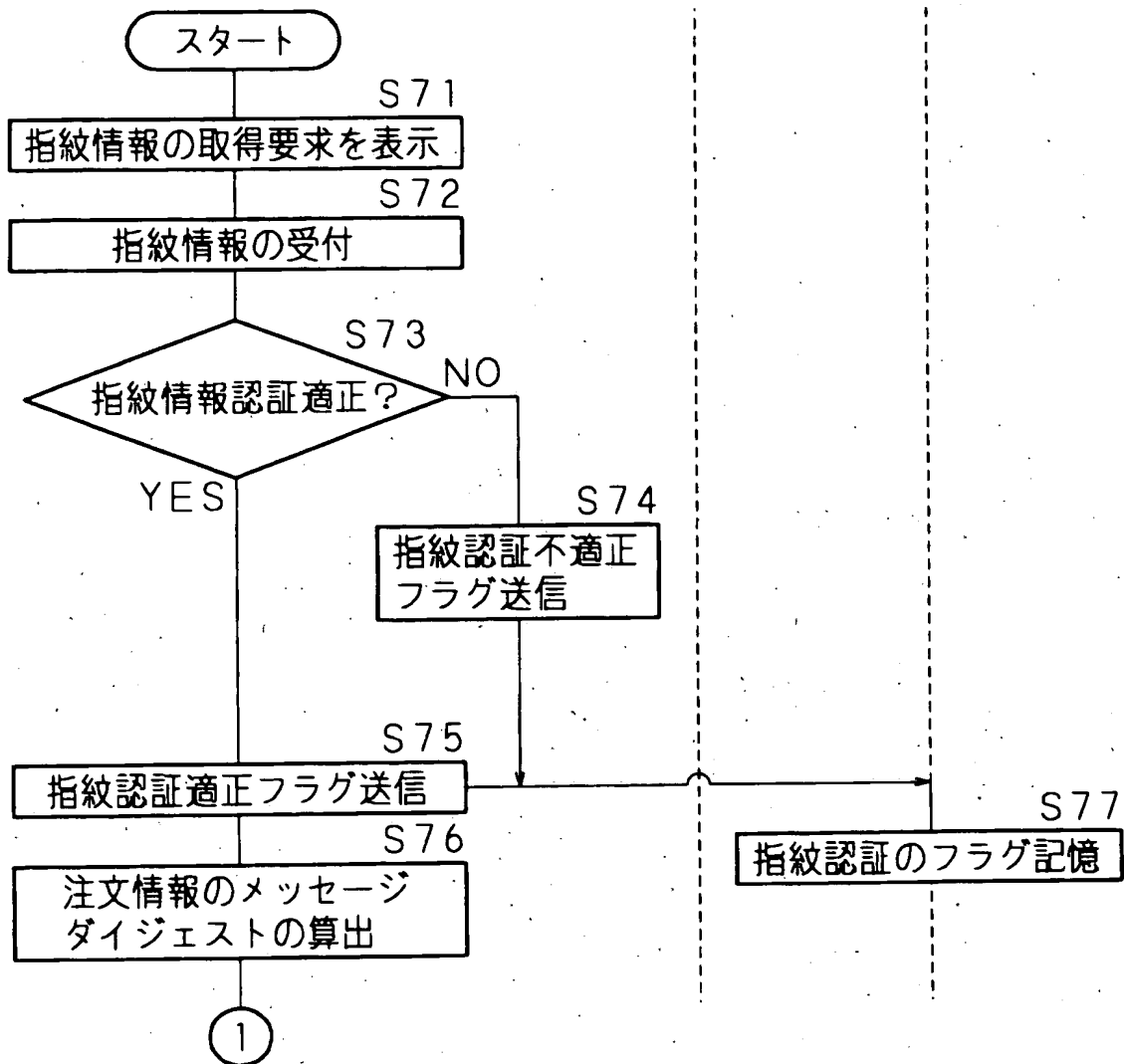
キャンセル

【図 7】

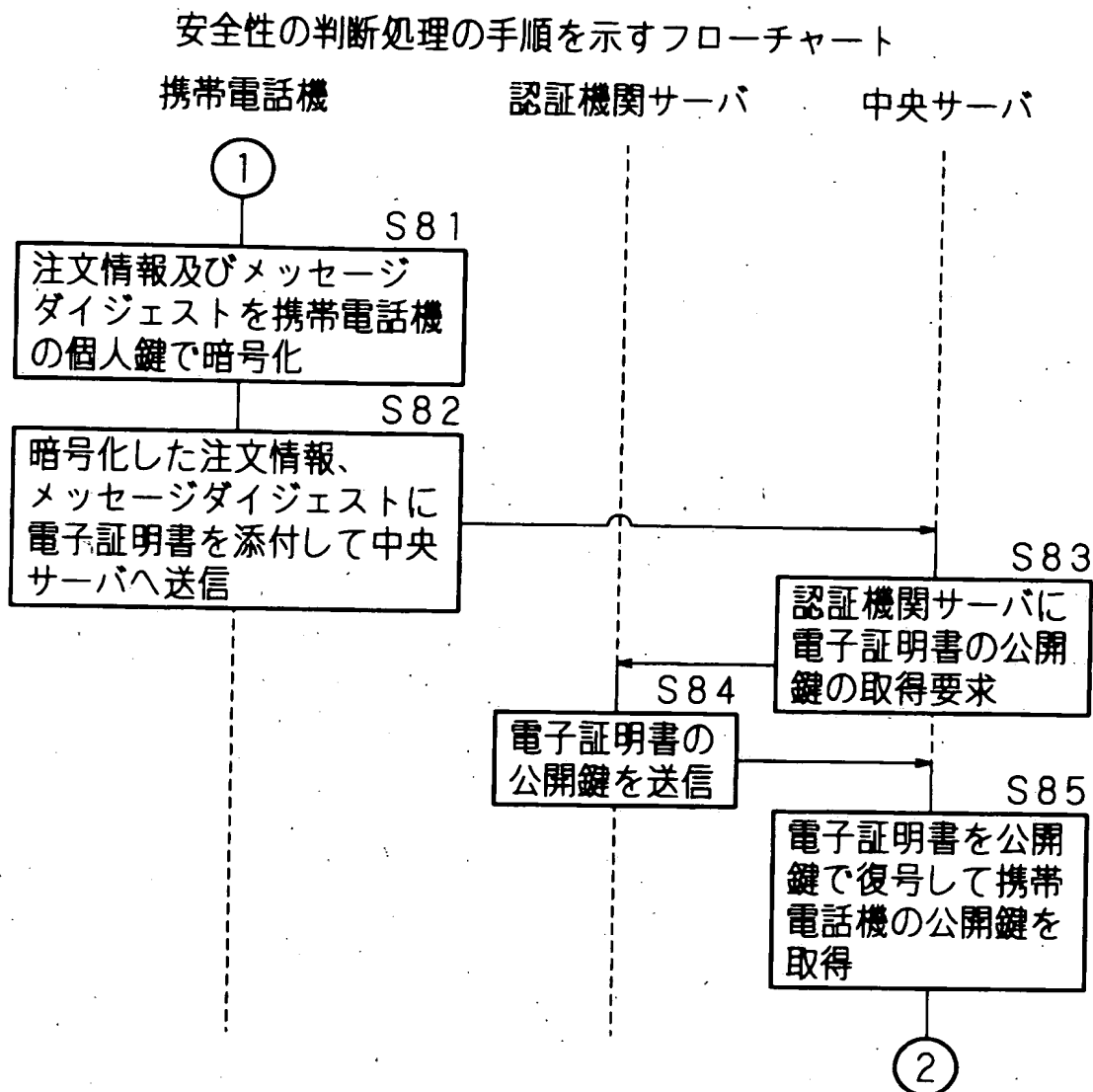
安全性の判断処理の手順を示すフローチャート

携帯電話機

認証機関サーバ 中央サーバ



【図 8】

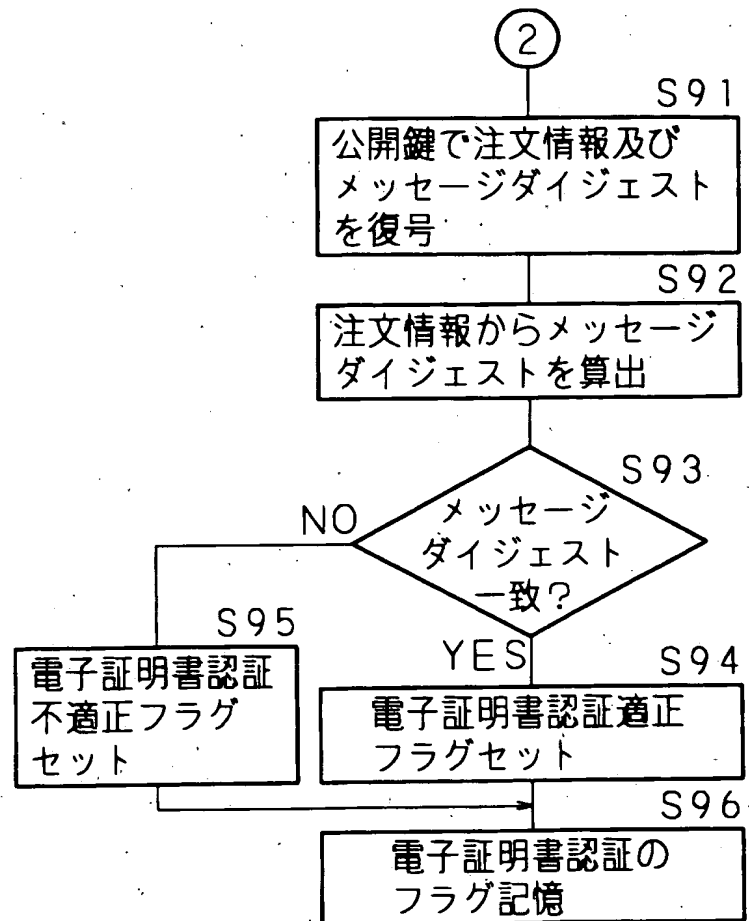


【図 9】

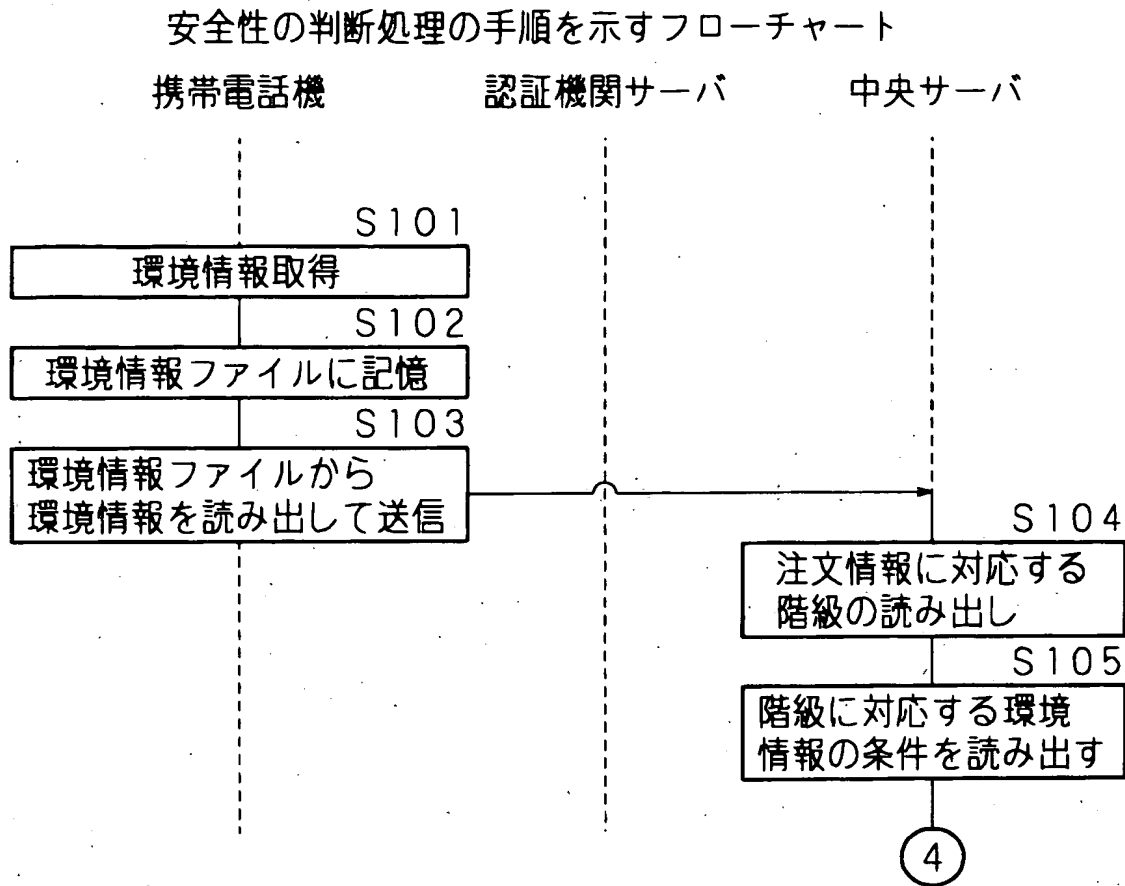
安全性の判断処理の手順を示すフローチャート

携帯電話機 認証機関サーバ

中央サーバ



【図 10】

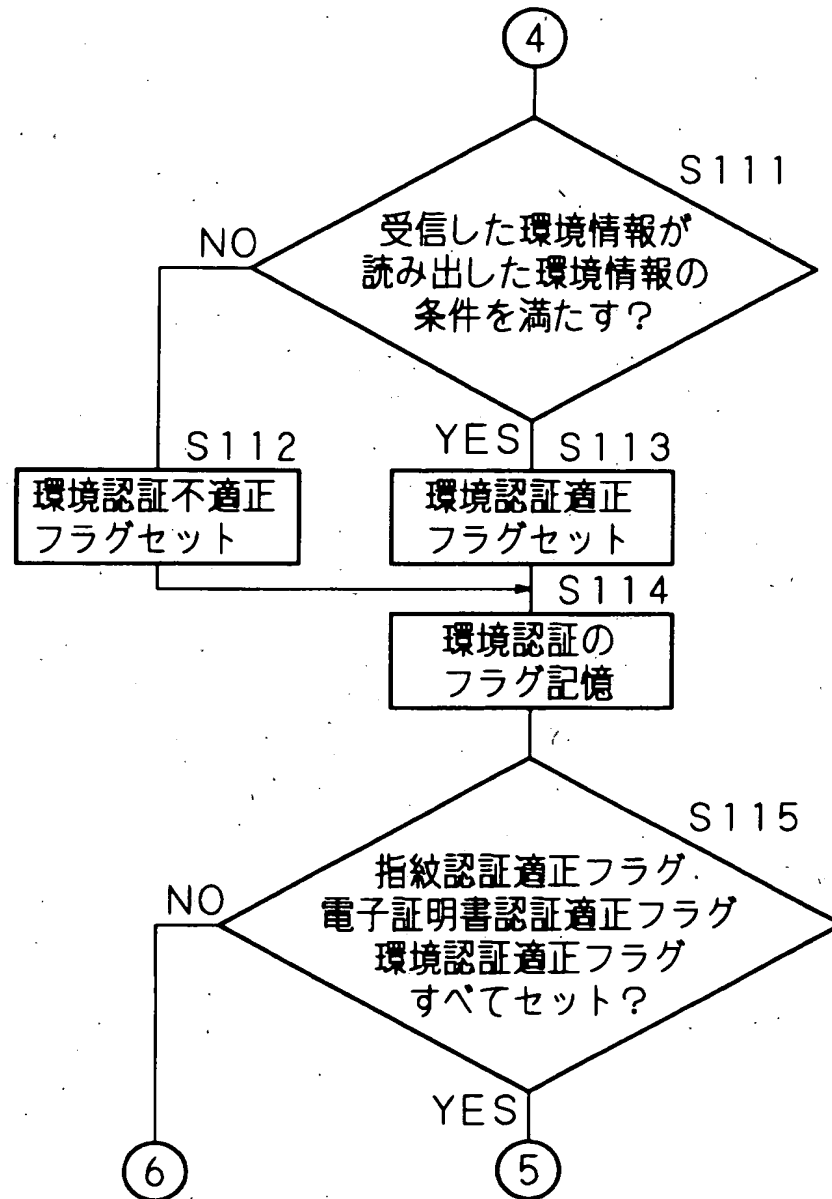


【図 11】

安全性の判断処理の手順を示すフローチャート

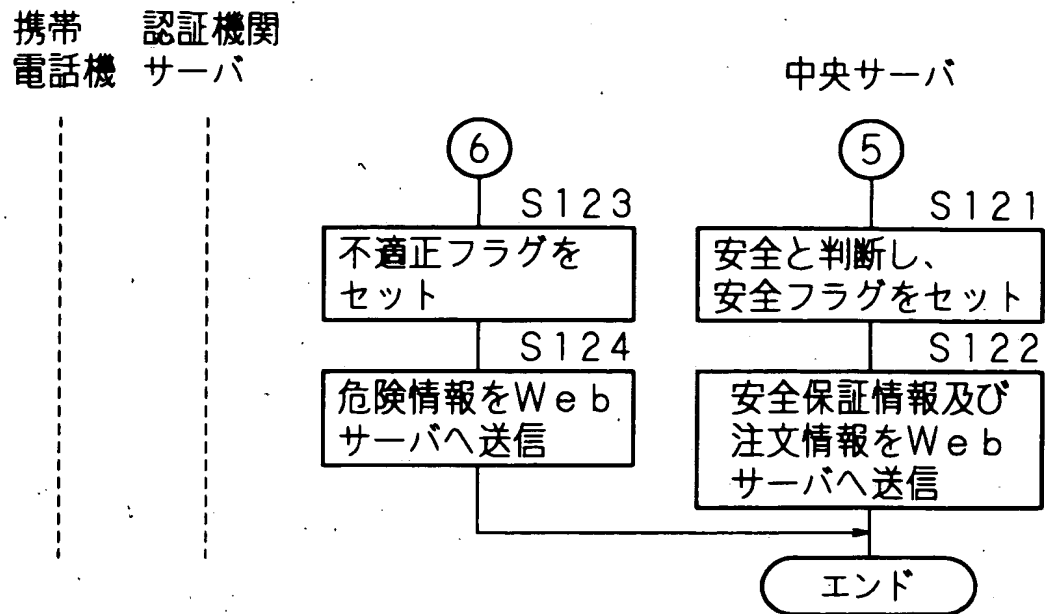
携帯 認証機関  
電話機 サーバ

中央サーバ



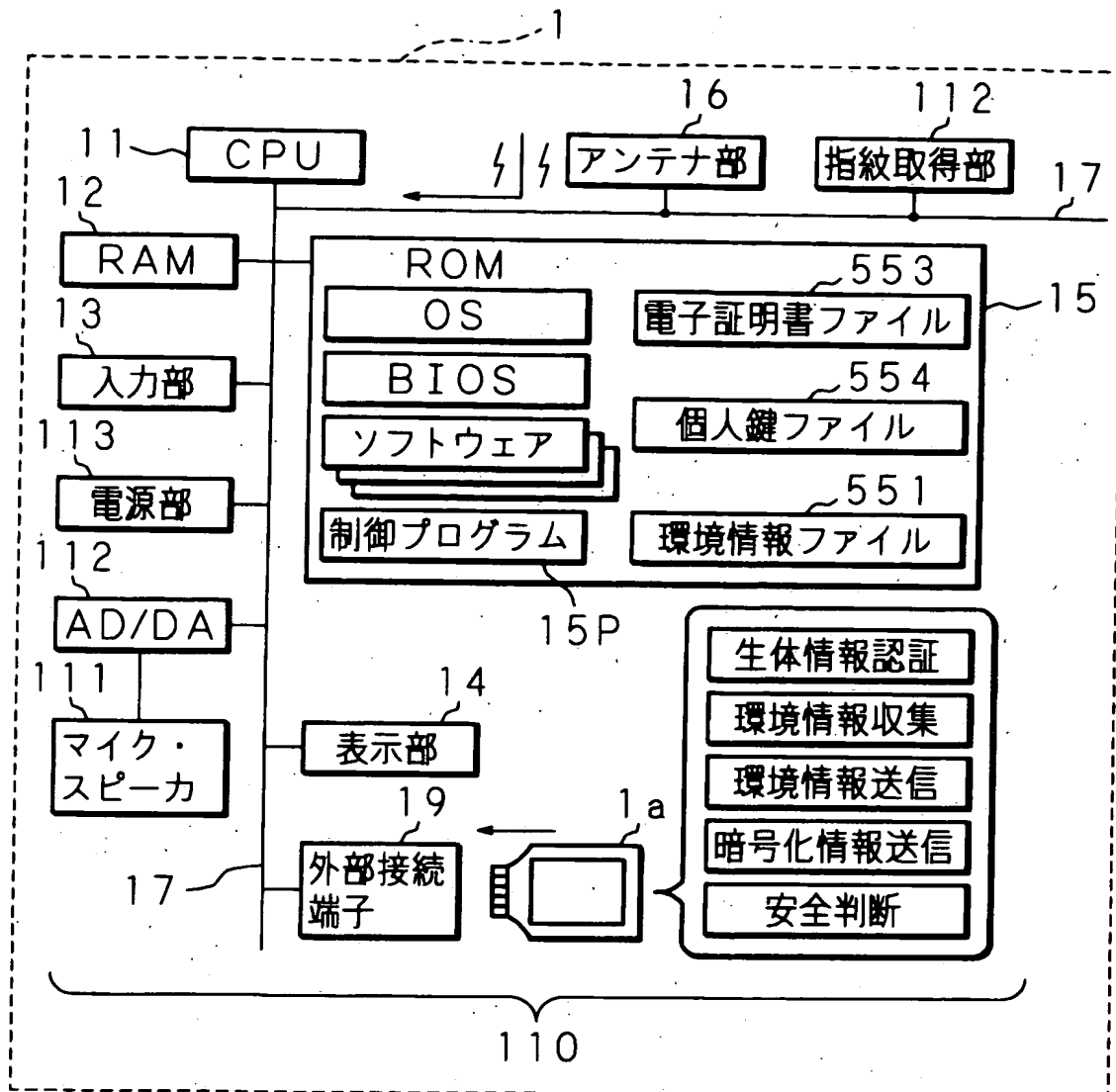
【図 12】

安全性の判断処理の手順を示すフローチャート



【図13】

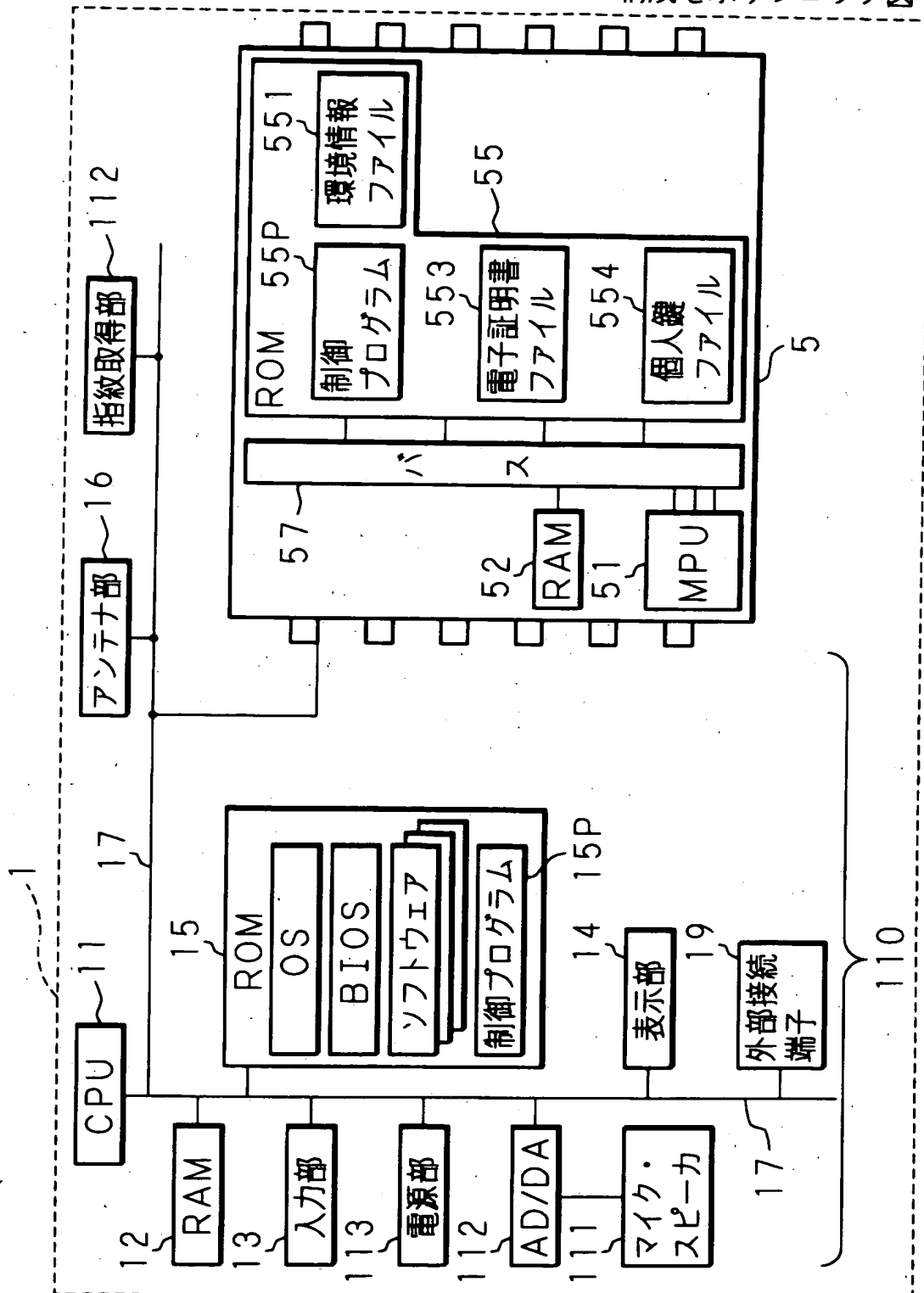
実施の形態2に係る携帯電話機のハードウェア構成を示すブロック図





【図 14】

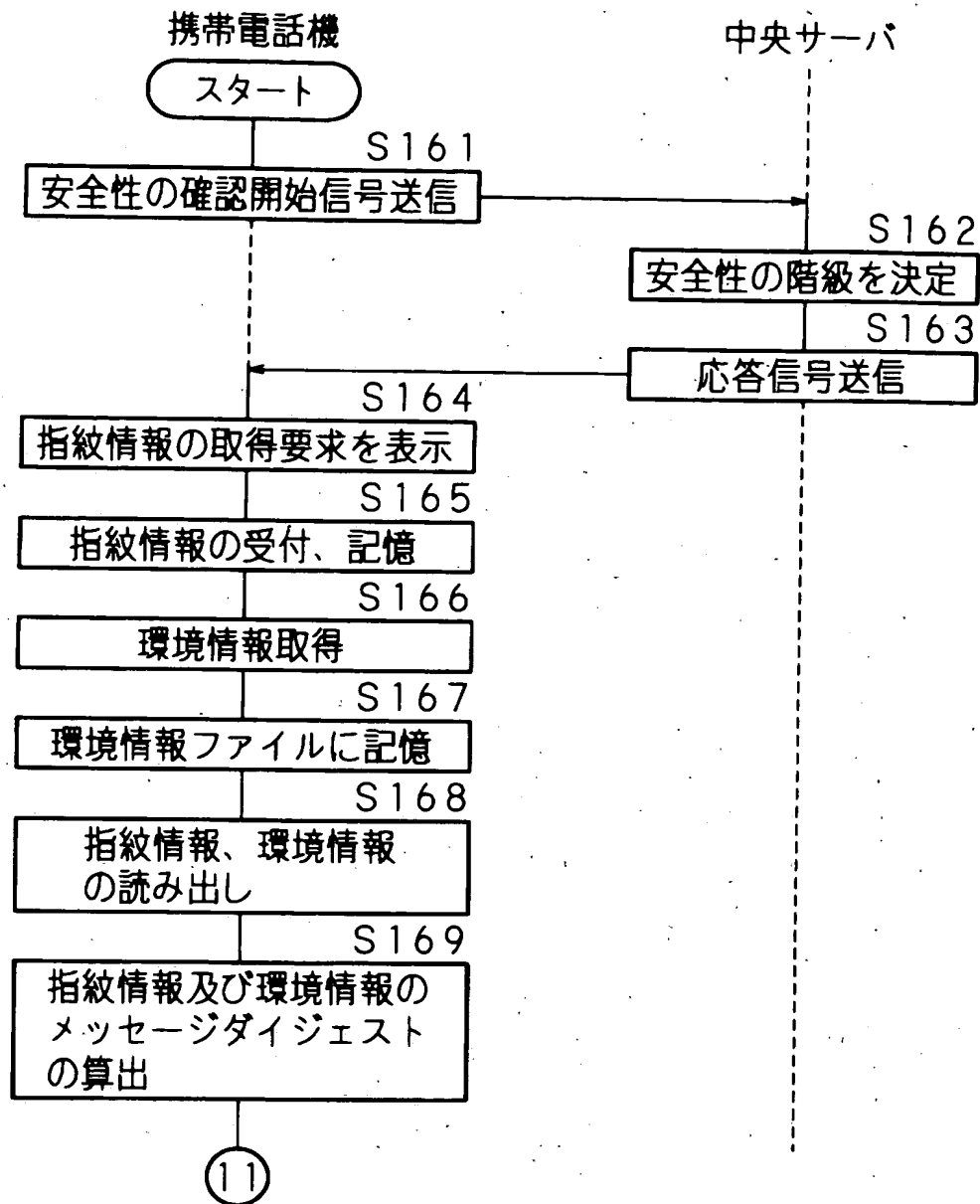
実施の形態 3 に係る携帯電話機のハードウェア構成を示すブロック図





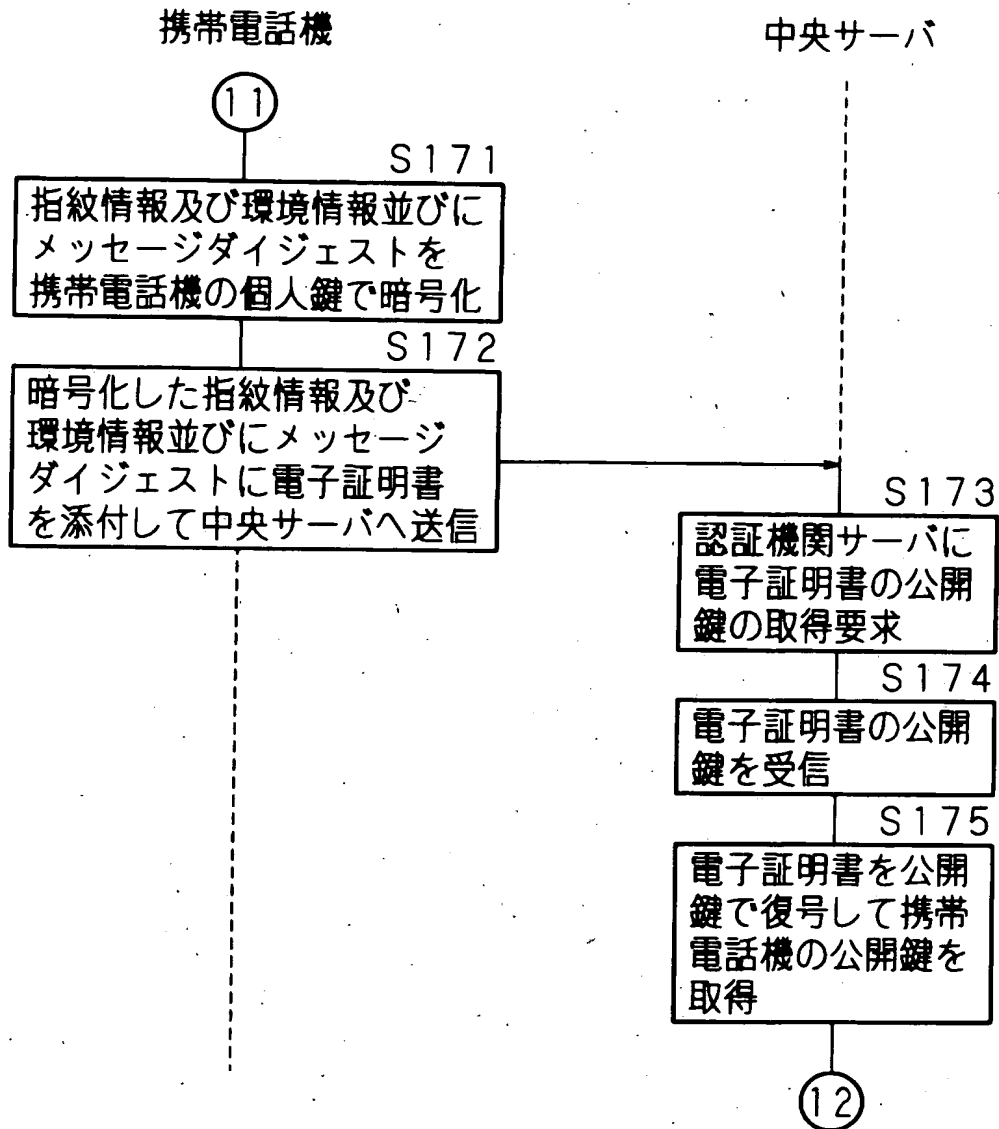
【図 16】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャート



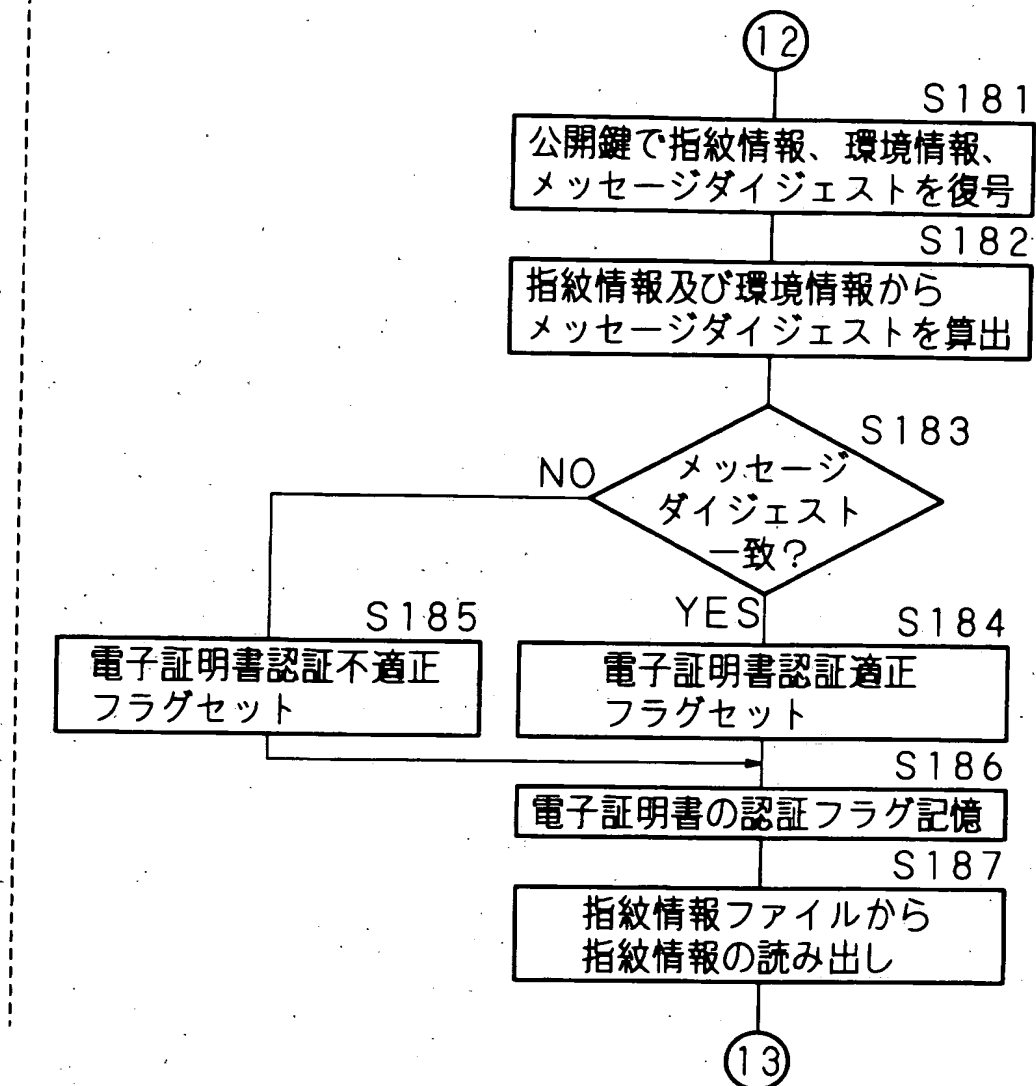
【図 17】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャート



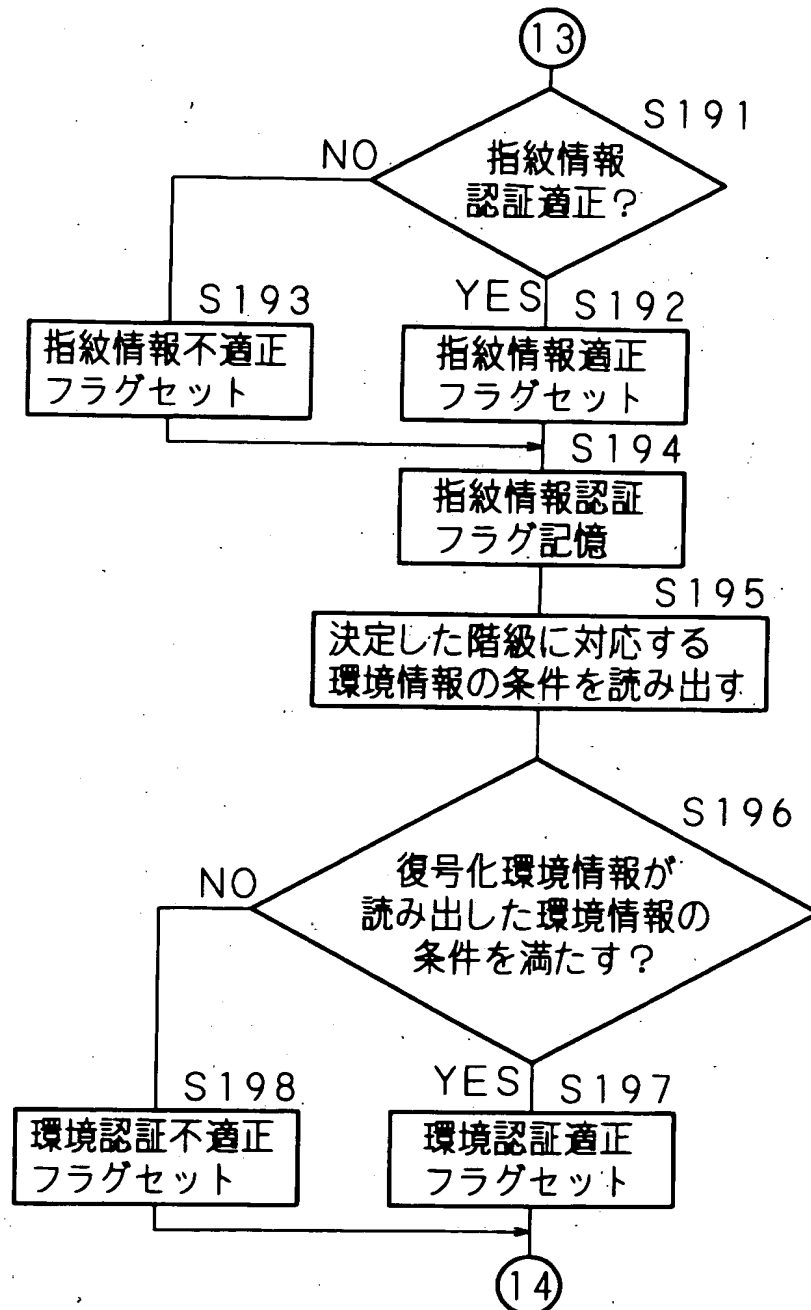
【図18】

実施の形態3に係る安全性の判断処理の手順を示すフローチャート  
携帯電話機 中央サーバ



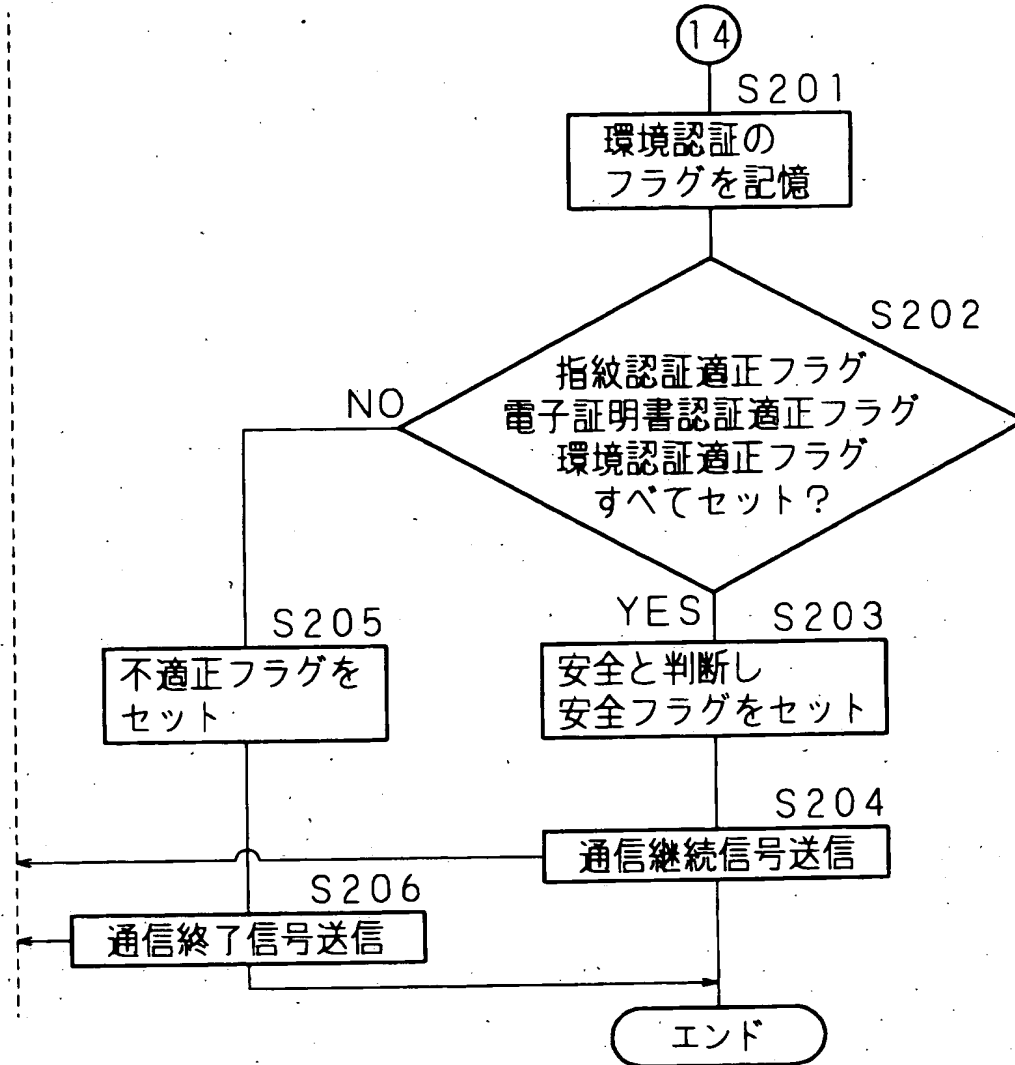
【図 19】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャート  
携帯電話機 中央サーバ



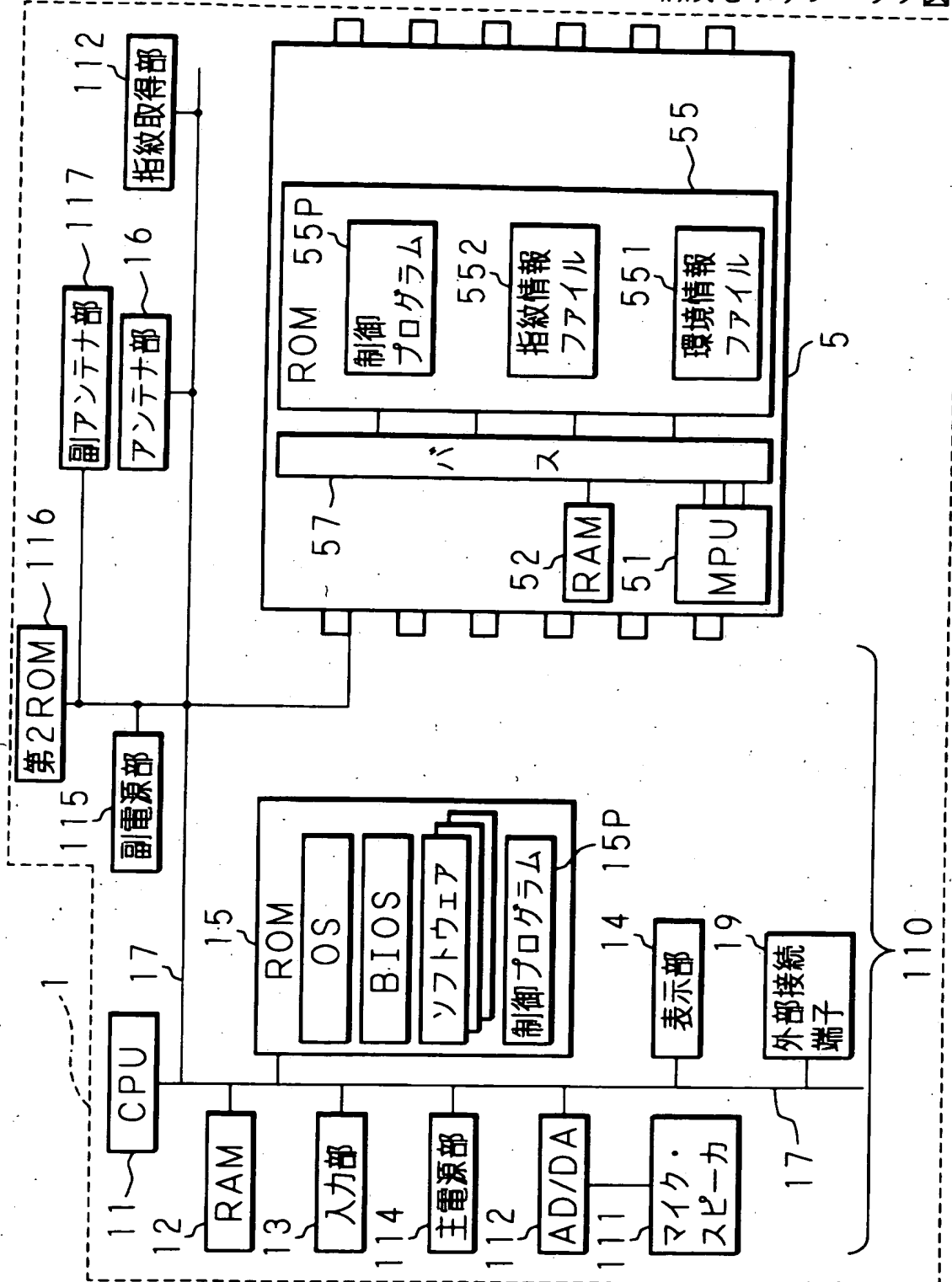
【図 20】

実施の形態 3 に係る安全性の判断処理の手順を示すフローチャート  
携帯電話機 中央サーバ



【図 21】

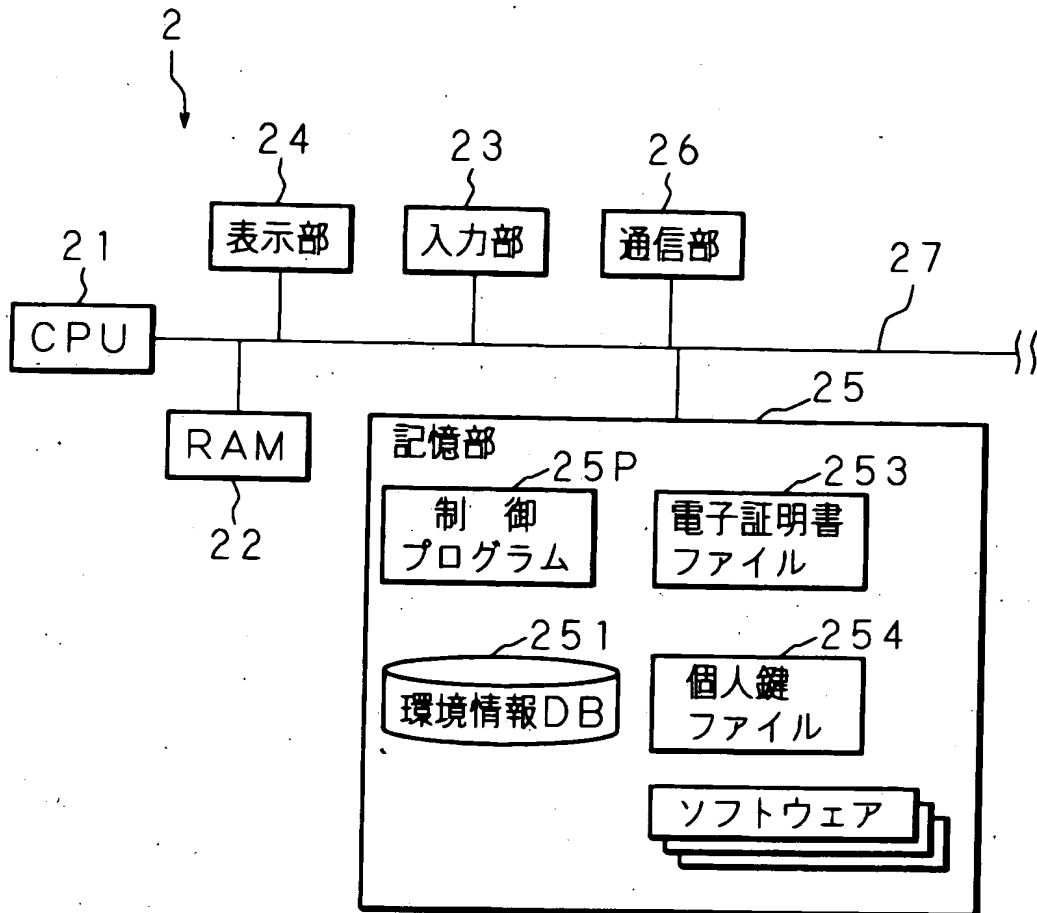
実施の形態 4 に係る携帯電話機のハードウェア構成を示すブロック図





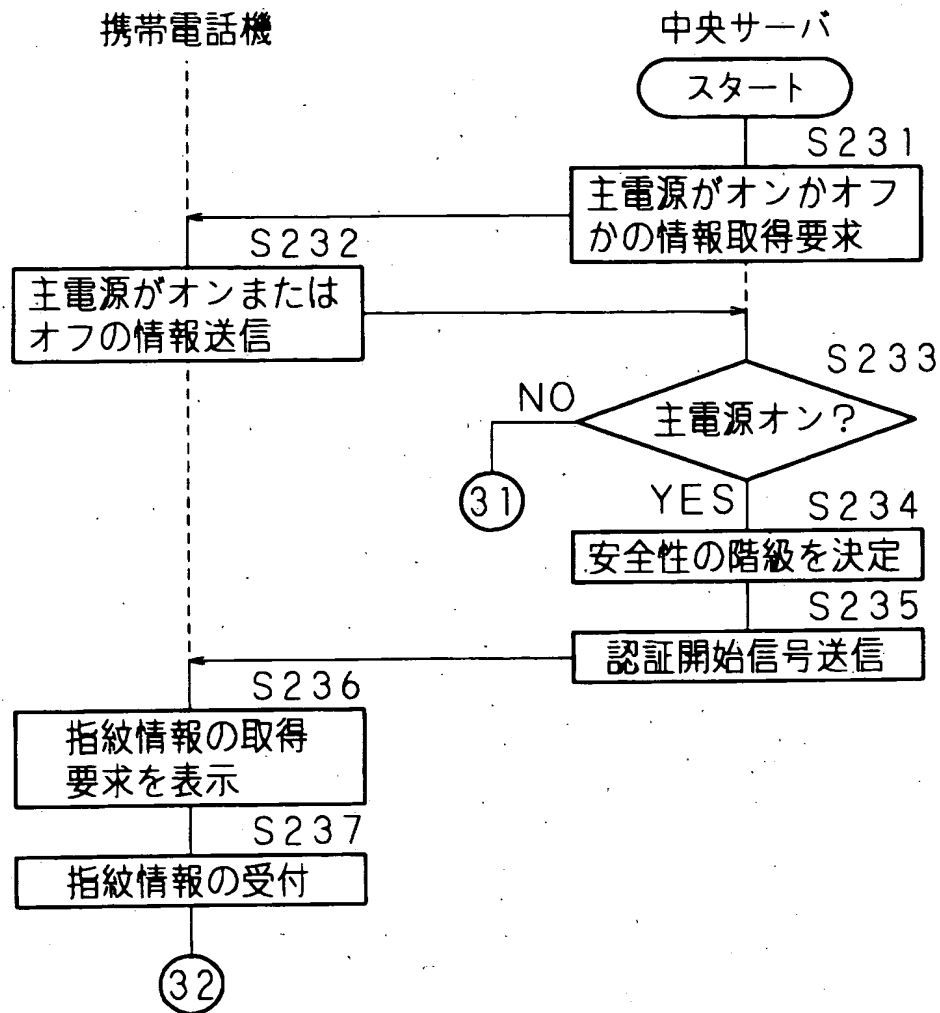
【図 22】

中央サーバのハードウェア構成を示すブロック図



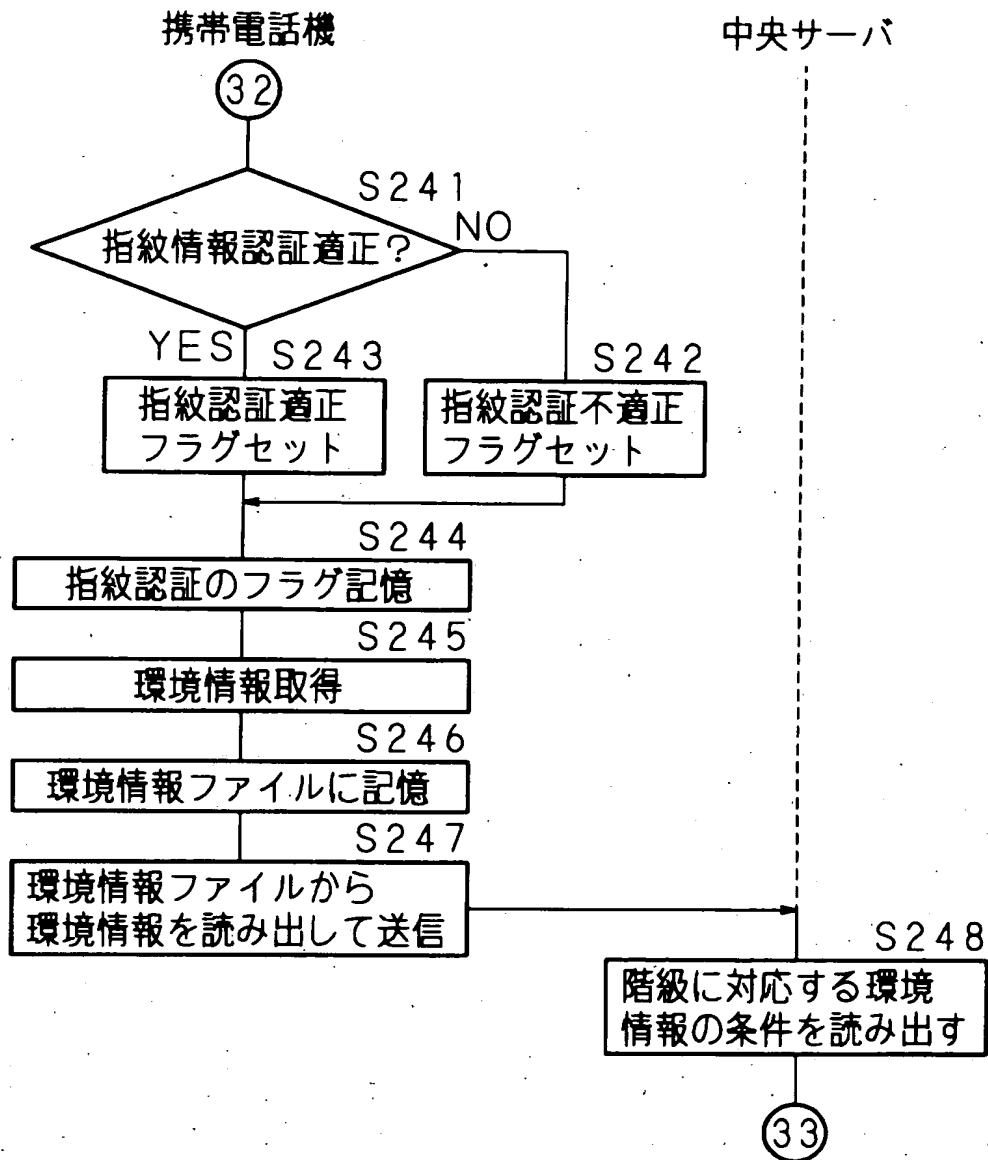
【図 23】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャート



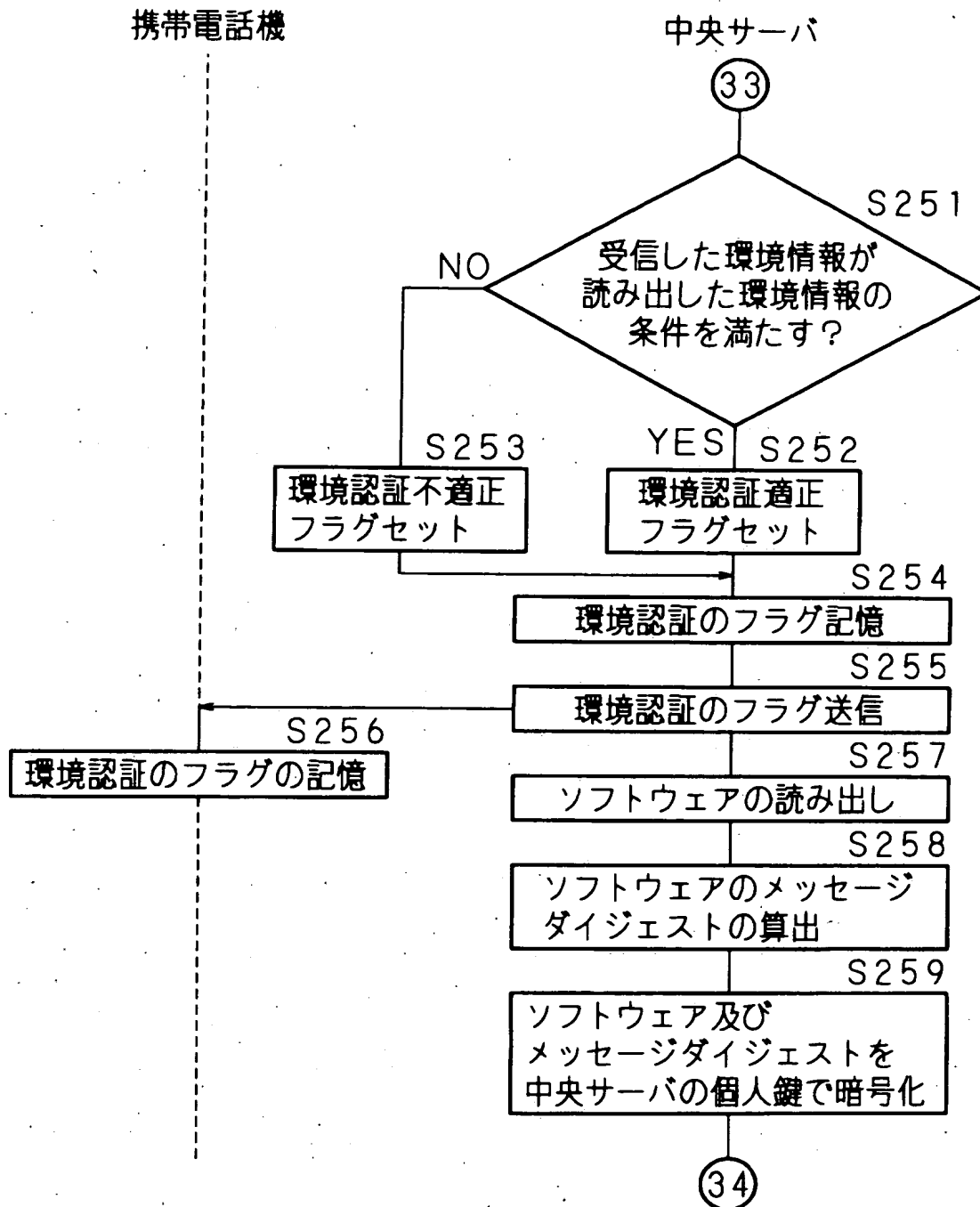
【図 24】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャート



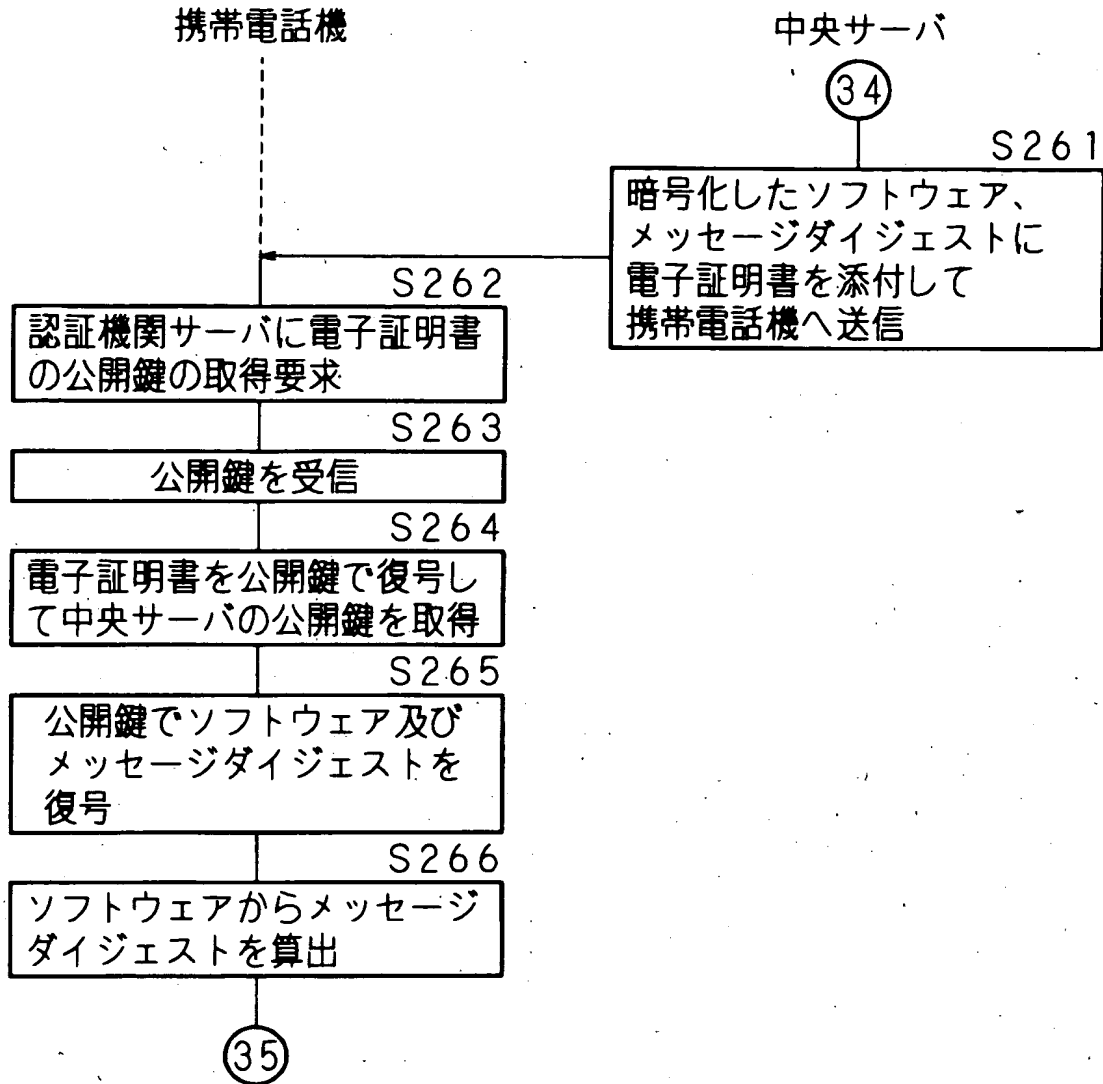
【図 25】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャート



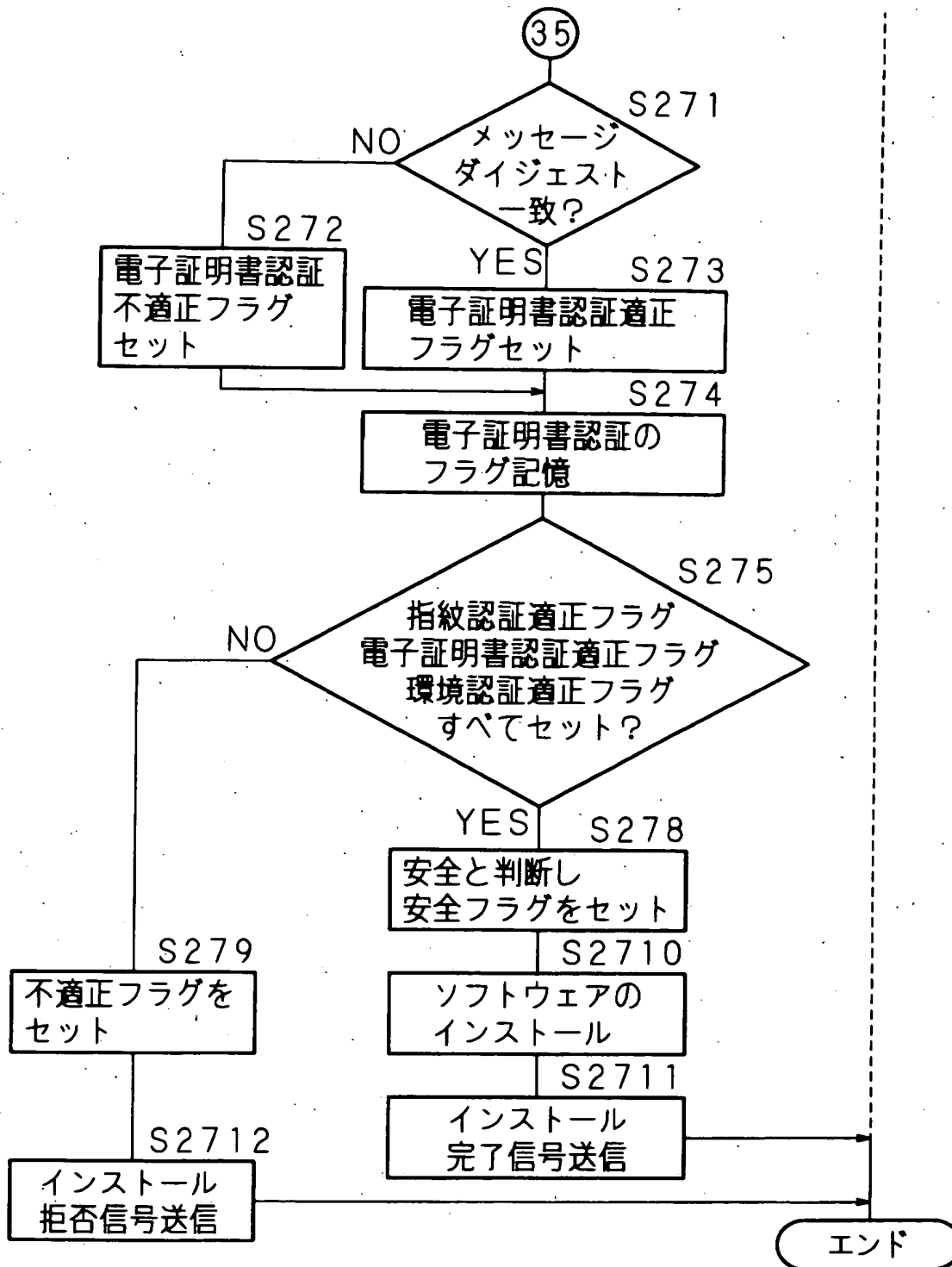
【図 26】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャート



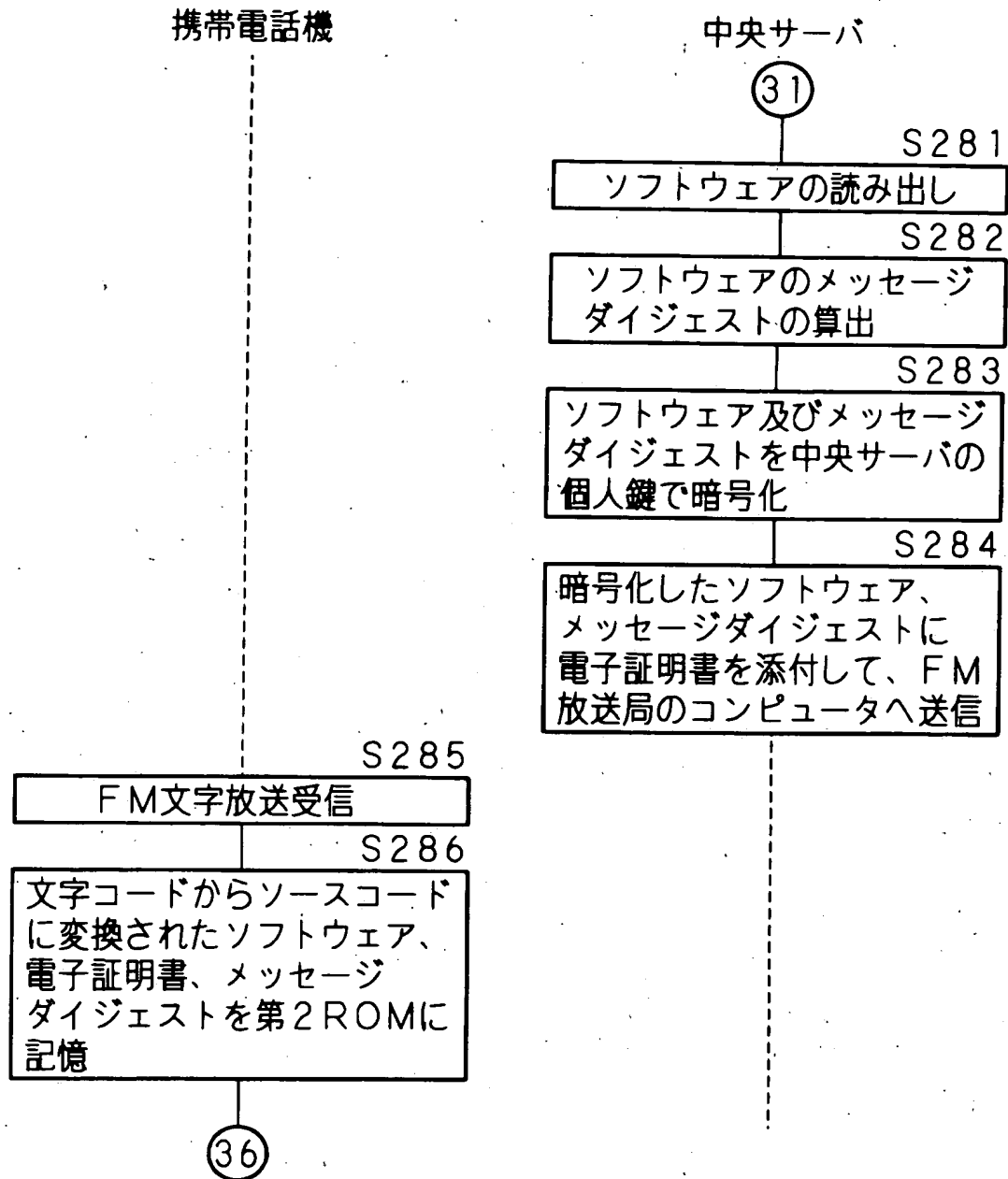
【図 27】

実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャート  
携帯電話機 中央サーバ



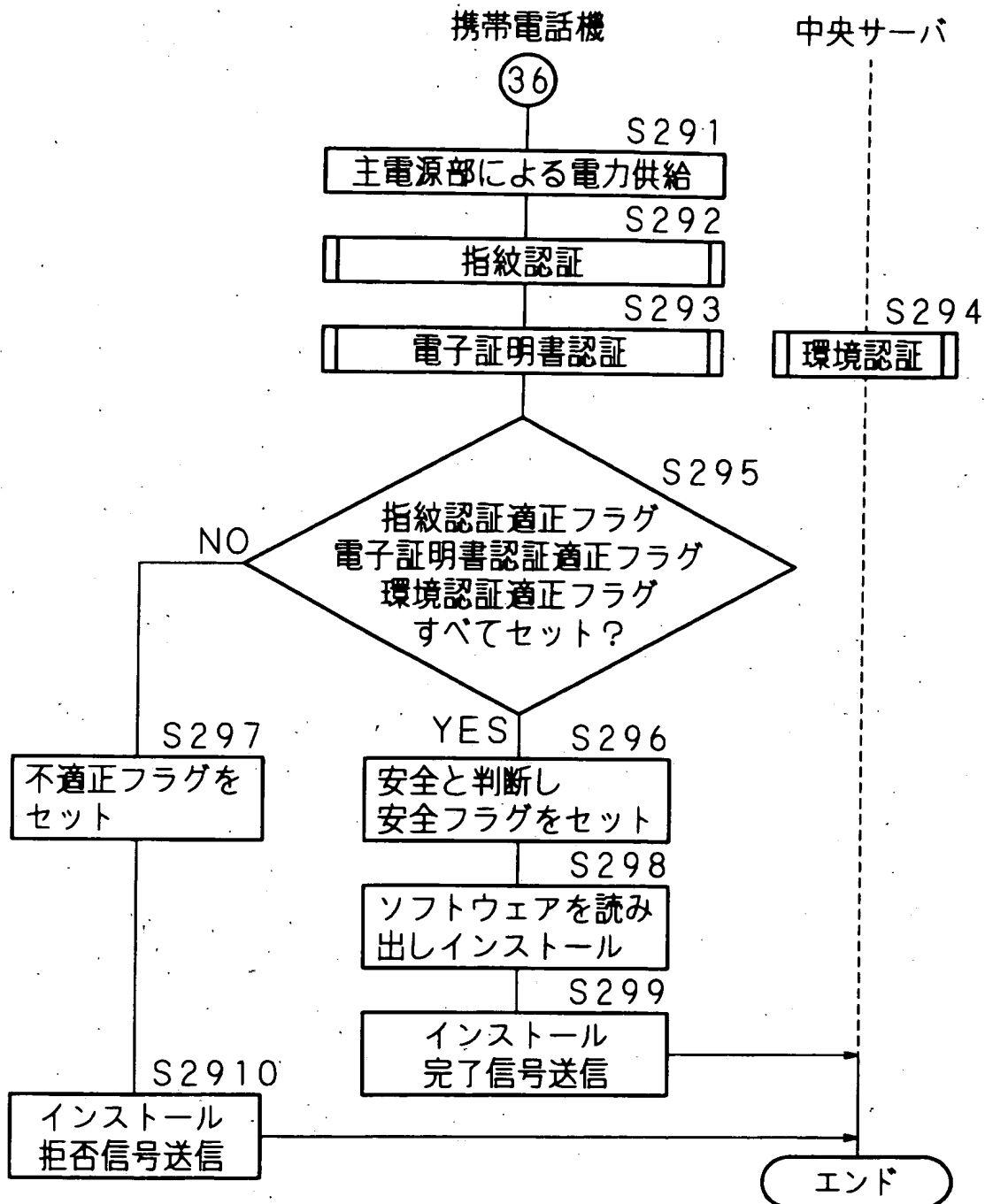
【図 28】

実施の形態 4に係るソフトウェア提供処理の手順を示すフローチャート



【図 29】

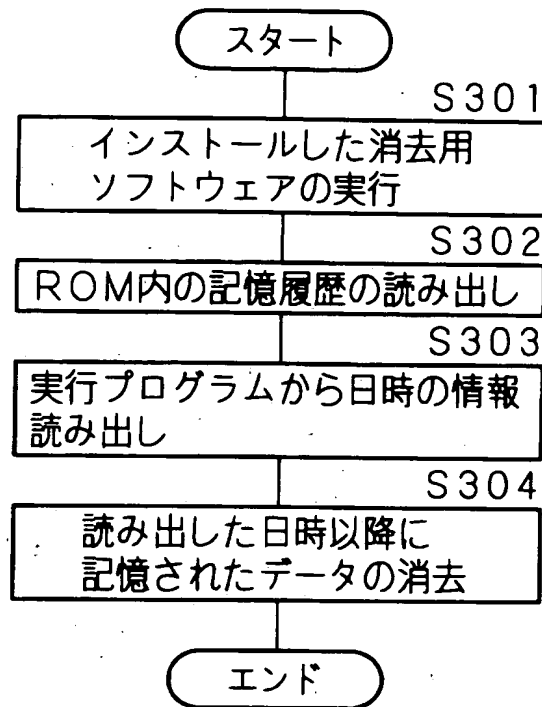
実施の形態 4 に係るソフトウェア提供処理の手順を示すフローチャート





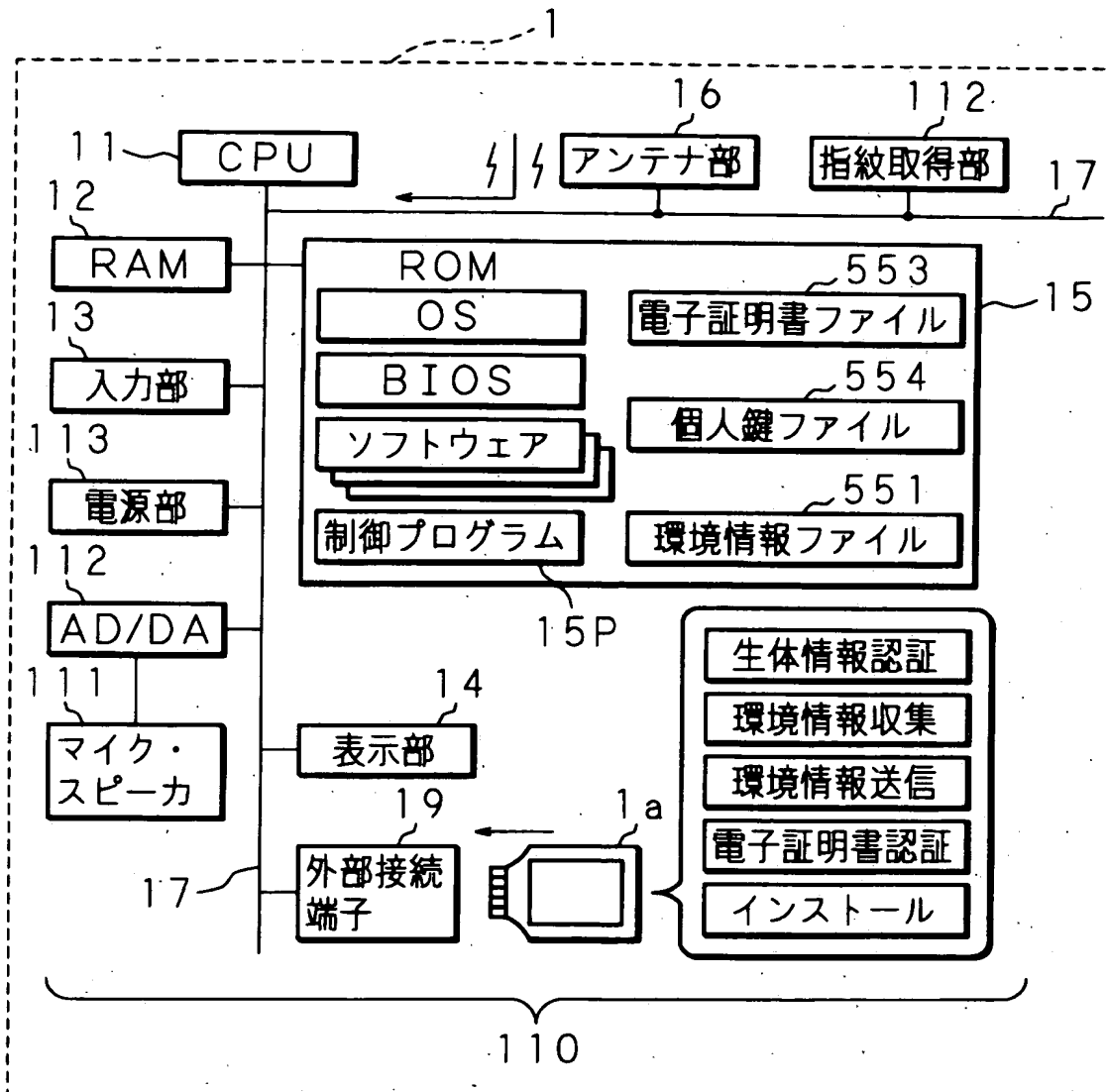
【図 30】

インストールされた消去用ソフトウェアの処理内容を示すフローチャート



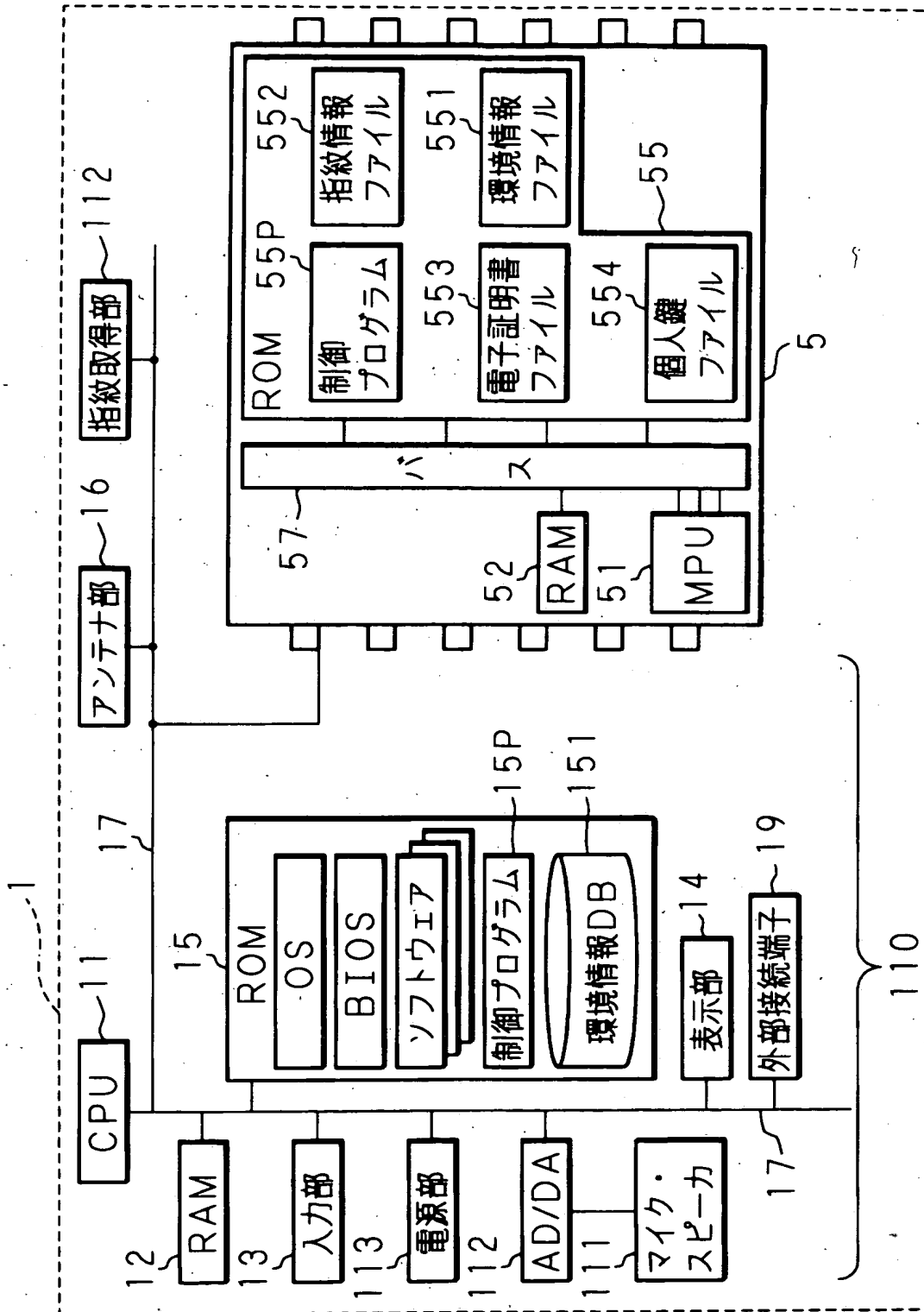
【図 3 1】

実施の形態 5 に係る携帯電話機のハードウェア構成を示すブロック図



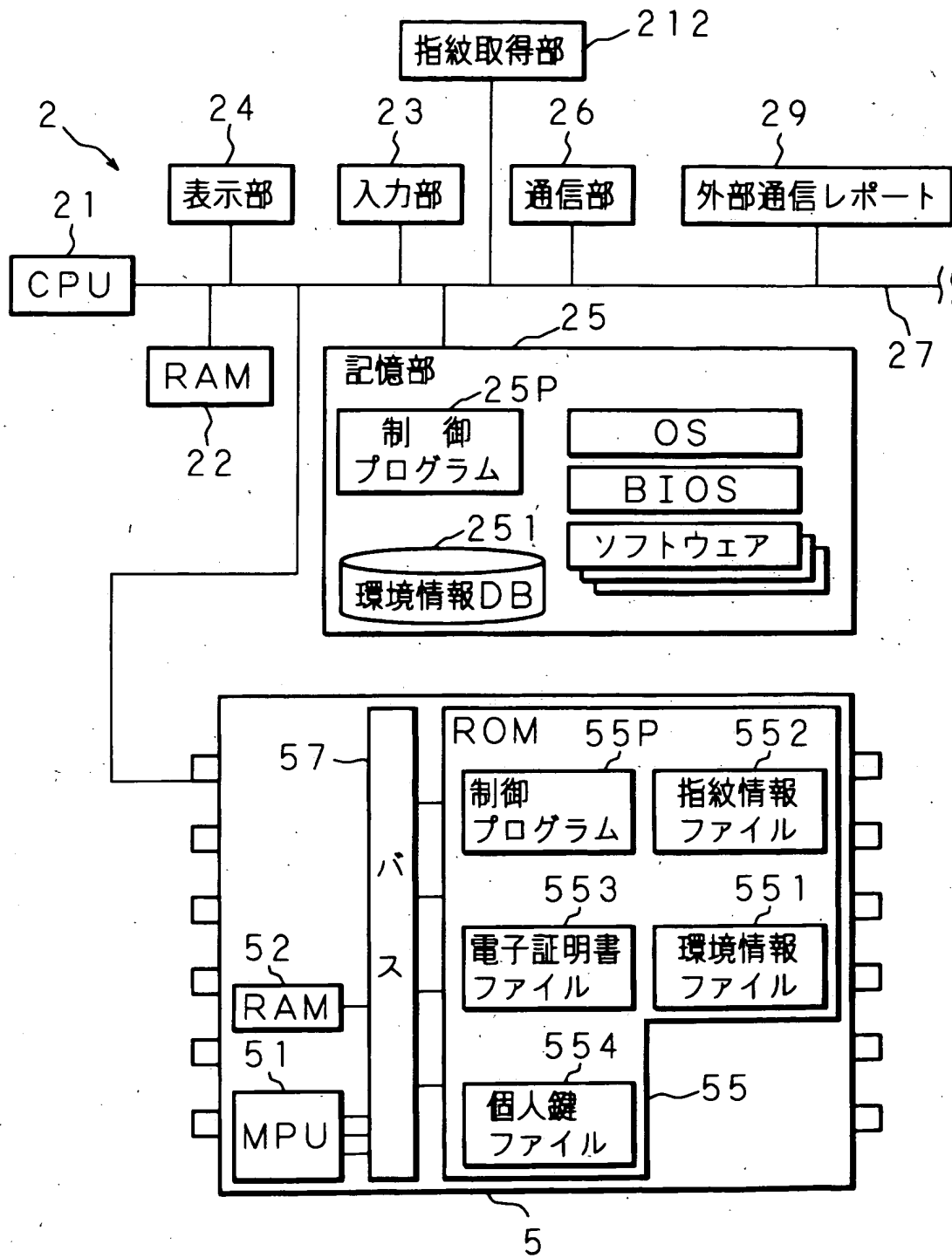
【図 3 2】

実施の形態 6 に係る携帯電話機のハードウェア構成を示すブロック図



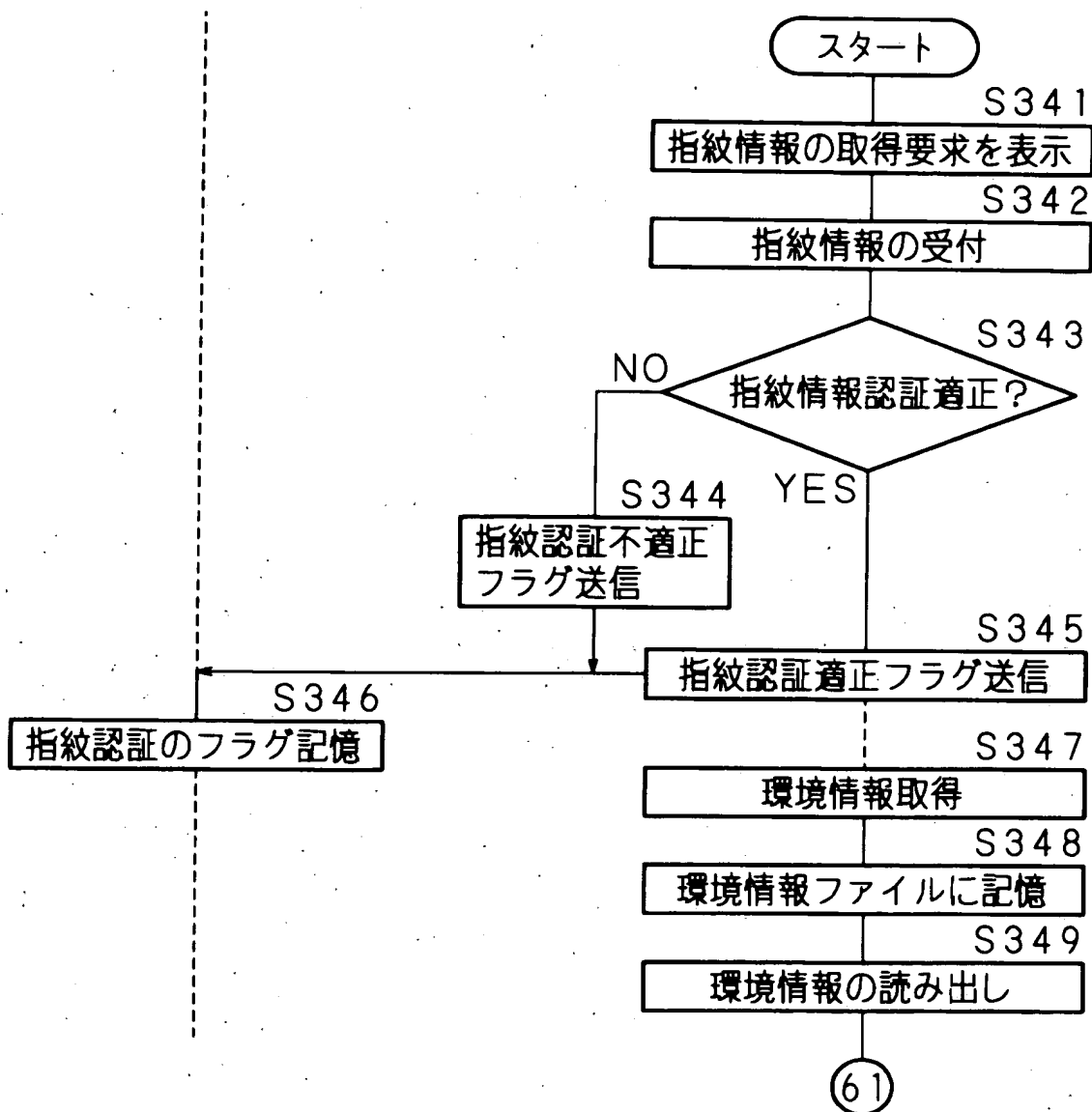
【図 33】

実施の形態 6 に係る中央サーバのハードウェア構成を示すブロック図



【図 34】

実施の形態 6 に係る認証処理の手順を示すフローチャート  
携帯電話機 中央サーバ

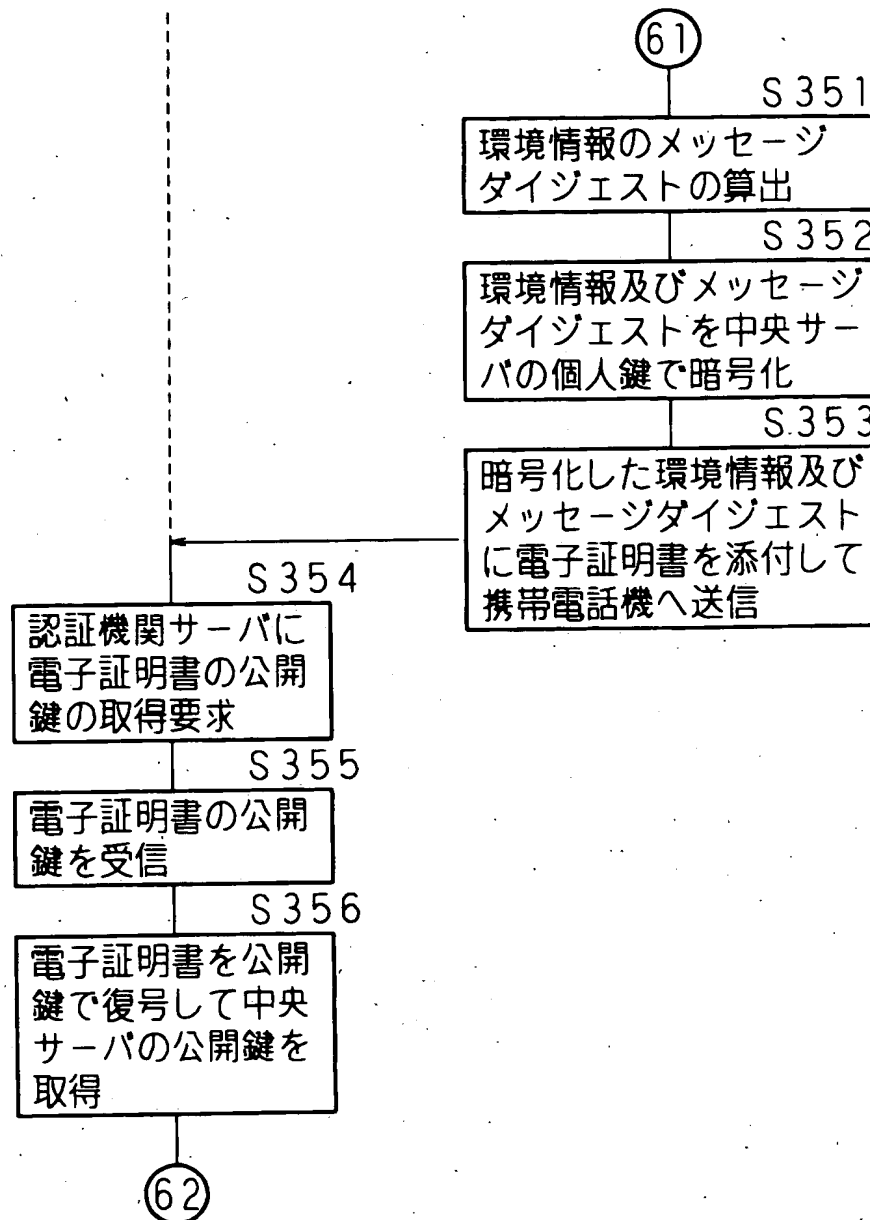


【図 35】

実施の形態 6 に係る認証処理の手順を示すフローチャート

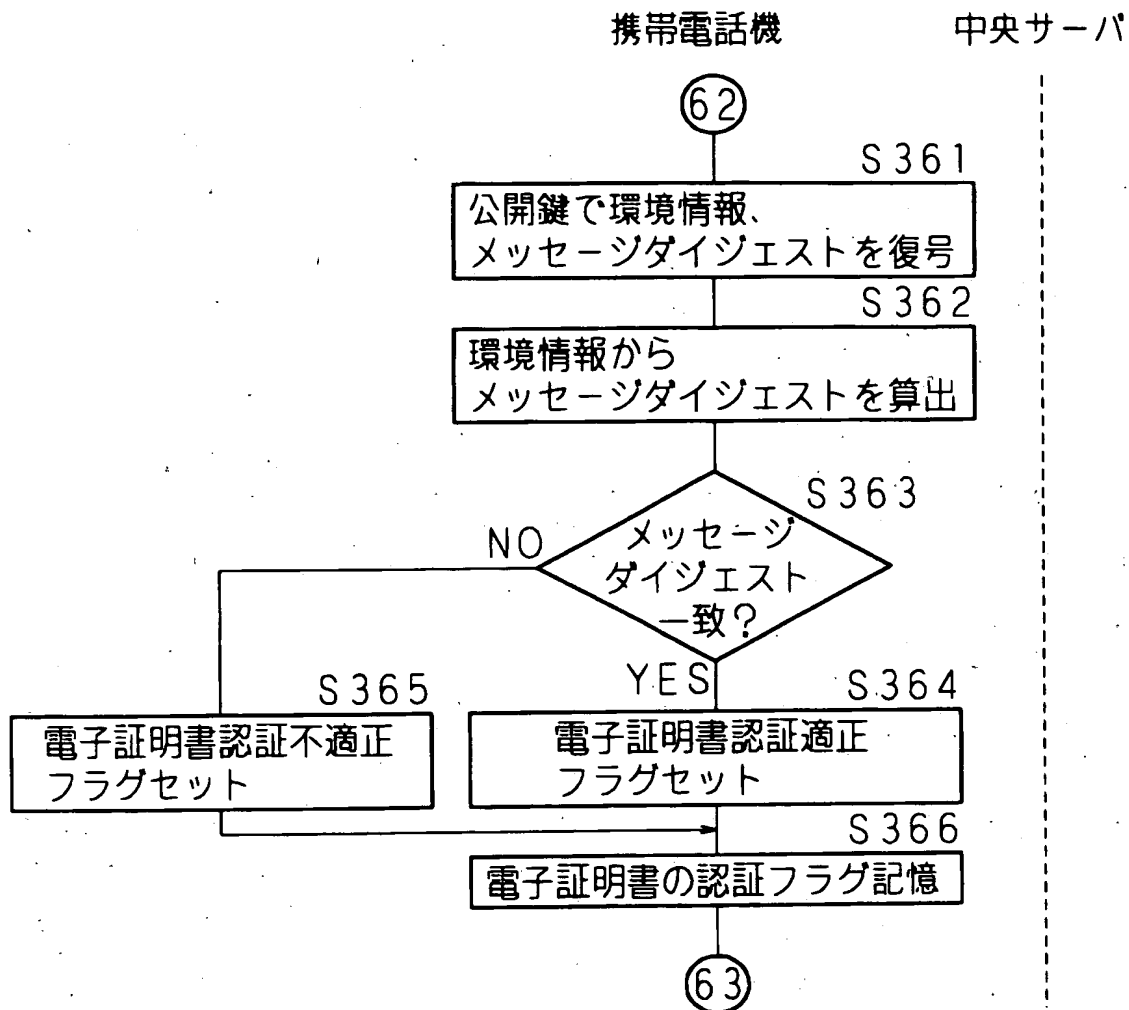
携帯電話機

中央サーバ



【図 36】

実施の形態 6 に係る認証処理の手順を示すフローチャート

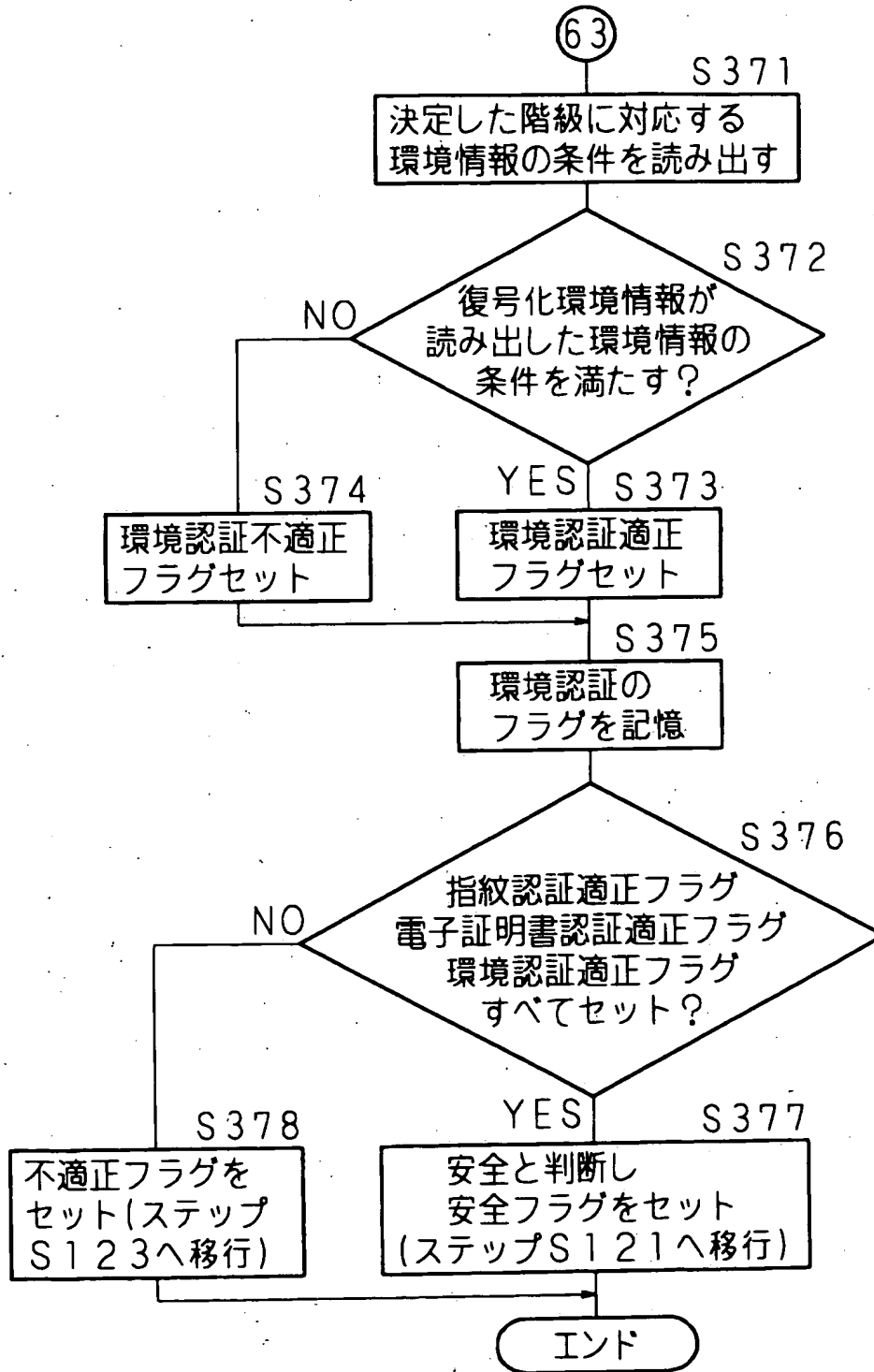


【図 37】

実施の形態 6 に係る認証処理の手順を示すフローチャート

携帯電話機

中央サーバ





【書類名】 要約書

【要約】

【課題】 安全性を高めることができ、また妥当な安全性を維持した上で円滑に情報の送受信を行うことが可能な安全性判断方法を提供する。

【解決手段】 生体情報認証を行い、また情報処理装置 1 の環境情報を収集する。情報処理装置 1 は収集した環境情報を第 1 認証装置 2 へ送信する。第 2 認証装置 3 から発行を受けた電子証明書及び個人鍵で暗号化された情報を第 1 認証装置 2 へ送信する。第 1 認証装置 2 は、第 2 認証装置 3 の公開鍵及び情報処理装置 1 の公開鍵を取得し、暗号化された情報を復号し、復号された情報が適正であるか否かを判断する。第 1 認証装置 2 は環境情報データベース及び送信された情報を参照して、送信された環境情報が適正であるか否かを判断する。生体情報認証、環境情報認証、及び電子証明書認証による認証が全て適正である場合に情報処理装置 1 を安全と判断する。

【選択図】 図 1

特願 2002-323200

出願人履歴情報

識別番号

[000005223]

1. 変更年月日 1990年 8月24日  
[変更理由] 新規登録  
住 所 神奈川県川崎市中原区上小田中1015番地  
氏 名 富士通株式会社
2. 変更年月日 1996年 3月26日  
[変更理由] 住所変更  
住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社